Cumhuriyetin
75' inci Yıldönümü Dizisi

Bilişim Yönetiminin Ve Teknolojisinin Denetimi

Çeviri

Bilişim Yönetiminin ve Teknolojisinin Denetimi

Çeviri

Cumhuriyetin 75'inci Yıldönümü Dizisi: 3

Özgün Adı: Auditing of Information Management and Technology

Kanada Sayıştayı tarafından yayımlanan (1994) kitapçığın İngilizce nüshasından dilimize aktarılmıştır.

Sayıştay mensuplarının kullanımı için basılmıştır.

Kapak Tasarımı : *Alper Alpay*

Redaksiyon : *Gülsün Canova*
Dizgi ve Mizanpaj : *Ümmühan Arslan*
Baskı ve Cilt : *Sayıştay Yayın İşleri Müdürlüğü*

Birinci Basım : *Aralık, 1998*

TC SAYIŞTAY BAŞKANLIĞI
06100 ULUS, ANKARA
Tlf: 310 23 00

Cumhuriyetin 75' inci Yıldönümü Dizisi'nden Yayımlanan Kitaplar

*Cumhuriyetin 75' inci Yılında Kamu Harcamaları ve Denetimi Sempozyumu/**Tebliğler, Panel ve Tartışmalar***

*Avrupa Birliği Sayıştayı/**İsmail Hakkı Sayın***

SUNUŞ

Bilişim Teknolojisi baş döndürücü bir hızla gelişmekte ve kamu hizmetlerinde kullanımı da aynı şekilde yaygınlaşmaktadır. Bugün gelinen noktada, kamu kurum ve kuruluşlarımız ürettikleri kamu hizmetlerinin gerektirdiği doğru kararları zamanında alabilmek için daha çok bilgi toplayıp, bunları gecikmeden analiz ederek yeni üretilen bilgileri karar alma süreçlerine dahil etmek zorundadırlar. Bu durum, kamu kurum ve kuruluşlarımızda da, Batı'daki benzerleri gibi, çok geniş veri tabanlarına dayalı Yönetim Bilişim/Bilgi Sistemleri kurulmasını gerektirecektir. Hal böyle olunca, kamu kurum ve kuruluşları, çok yakın bir gelecekte, Bilişim Teknolojisine daha da bağımlı hale gelecektir.

Bu etkileşimin doğal bir sonucu olarak, Bilişim Yönetimi ve Teknolojine kamu fonlarından ayrılan paylar da giderek büyümekte, kamusal işlerin yürütülmesi gitgide artan ölçüde Bilişim Teknolojisine dayandırılmaktadır. Gerek ayrılan fonların doğru bir şekilde harcandığından, gerekse kurumlarca geliştirilen sistemler içinde, amaca uygun ve yeterli bilgiyi doğru, zamanlı ve ekonomik maliyetle üretebilecek etkili ve uygun kontrollerin kurulduğundan emin olmak gerekliliği, Bilişim Yönetimi ve Teknolojisi alanının denetlenmesi sonucunu doğurmaktadır.

Çizilen bu çerçevede Kanada Sayıştayı tarafından kendi mensuplarının kullanımı için hazırlanan bu denetim rehberinin "*Cumhuriyetin 75'inci Yıldönümü Dizisi*" arasında yayımlanan çevirisinin, Bilişim Yönetiminin ve Teknolojisinin denetimi çalışmalarında hem meslek mensuplarımıza ve hem de kamu kesimindeki diğer denetim elemanlarına yol gösterici olacağına inanıyorum.

Bu vesileyle, çevirinin meslekî üslûp ve terminoloji yönünden redaksiyonunda emeği geçen Uzman Denetçi Gülsün Canova ile kitabın dizgi, mizanpaj ve basımında görev alan mensuplarımıza teşekkür ederim.

Prof. Dr. M. Kâmil MUTLUER
Başkan

ÖNSÖZ

REHBERİN AMACI

Bu doküman; kurumlarında Bilişim Yönetimi ve Teknolojisinin denetimi yapacak denetçilere yol göstermek amacıyla hazırlanmıştır. Bu nedenle, Performans Denetimi ve diğer denetim hedefleri de, denetçinin Bilişim Teknolojisi bulgularının önemini kavraması ve denetimin çalışma alanını belirlemesi amacıyla doküman kapsamına alınmıştır. Bu rehbere, program denetimlerine ilişkin bilişim sistemleri incelenirken, bilişim sistemleri ile ilgili riskler değerlendirilirken ve Bilişim Yönetimi Hizmetleri bölümünün denetimini planlanırken baş vurulmalıdır.

GELİŞİMİN TEMELİ

Bu rehberin içeriği, geçmiş denetim çalışmalarına ve konuyla ilgili literatürün incelenmesine dayandırılmış ve bilişim teknolojisi alanında çalışan kişilerle yapılan mülakatlarla zenginleştirilmiştir. Bu dokümanı hazırlayanlar, katkıda bulunan herkesin yararlı fikirlerine ve önerilerine teşekkür ederken, tüm hataların ve atlanan hususların sorumluluğunu üstlenmektedirler.

YETKİ VE UYGULAMA

Bu rehber, alan testlerinden sorumlu Metodoloji Geliştirme Komitesi tarafından verilen yetkiyle, mevcut Bilgi İşlem rehberlerinin yerini almak amacıyla çıkarılmıştır. Rehber, Kapsamlı Denetim El Kitabıyla birlikte kullanılmalıdır. Rehberin içeriği bağlayıcı değildir ve denetim sorumlusunun profesyonel kararının yerine geçmek amacıyla da hazırlanmamıştır. Danışma faaliyeti, Kapsamlı Denetim Rehberi (KDR) 6011-6031 de öngörülmektedir. Bu rehberin kullanıcıları, alan testi tecrübelerini Profesyonel Çalışma Grubuna aktarmak suretiyle gelişimine katkıda bulunabilirler. Denetim sorumluları rehber içindeki bilginin nerede ve ne derecede kullanılacağına kendileri karar vermelidirler.

REHBERDE BENİMSENEN YAKLAŞIM

Bu rehber; denetçilere denetleyecekleri kurumlarda, Bilişim Teknolojilerine ilişkin riskleri değerlendirmede yardımcı olabilmek amacıyla bir çerçeve sunmaktadır. Teknoloji çok hızlı bir biçimde ilerlediğinden, Kurumumuz kendi metodolojisini geliştirme yerine, mevcut metodolojileri bir araya getirmeyi ve Bilişim Teknolojisine denetim rehberliği sağlamayı tercih etmiştir. Bu yaklaşım pahalıya malolan mükerrer gayretleri engellemekte ve rehberin daha zamanlı bir şekilde değerlendirilmesine olanak vermektedir. Rehberde en fazla yararlanılan çalışmalardan ikisi; İç Denetçiler Araştırma Enstitüsü'nün "Sistemlerin Denetlenebilirliği ve Kontrol" raporu ile Bilgi İşlem Denetçileri Kurumu'nun "Kontrol Hedefleri" isimli dokümanıdır.

Rehberin alan testine ilişkin versiyonu bazı risk değerlendirme faktörlerini içermektedir ancak genel kapsamlı bir Bilişim Teknolojileri risk değerlendirmesi modeli oluşturmamaktadır. Böyle bir çerçeveyi geliştirerek gelecekte yapılacak rehberliğe dahil etmek düşüncesindeyiz.

REHBERİN KAPSAMI

Rehberin ilk bölümü; günümüzde kamu kurumlarında var olan bilişim teknolojisi ortamı hakkında kısa bilgiyi içermektedir. Ayrıca, Bilişim Yöneticisinin görevini belirtirken bilişim denetiminin gereğini de vurgulamaktadır.

İkinci bölüm; bilişim teknolojisinin kurum tarafından yeterli derecede değerlendirilip değerlendirilmediğini tesbit etmek üzere, kurum çalışmaları hakkında bilgi edinilmesini sağlayacak geniş çerçeveyi sunmaktadır. Ayrıca telekomünikasyon denetimi dışında Hazine Kurulunun bilişim yönetimi politikaları, güvenlik ve destek faaliyetlerine uygunluk konularına da eğilmektedir. Bilişim Teknolojilerinin esas maliyetleri konusundaki değerlendirme de bu bölümün son kısmında yer almaktadır.

Üçüncü bölüm; önceki bölümü daha da genişleterek bir program değerlendirme denetimi çerçevesinde bilişim teknolojilerinin denetimini işlemektedir. Bu bölüm program denetçileri tarafından incelenmesi gereken anahtar alanları tanımlamaktadır.

Dördüncü bölüm; tastik denetimine ilişkin konuları ve uygulamaya ilişkin değerlendirmeleri içermektedir. Üzerinde durulan iki konu, sistem kontrolleri ve bölümlere ayrılan işlemelerdir (proceedings). Anahtar sistem kontrolleri, denetçilere temel kavramları sunmak amacıyla rehbere dahil edilmişlerdir. Bu bölüm rehberin bir sonraki baskısında daha da genişletilecektir.

Beşinci bölüm, Bilişim Teknolojilerine ilişkin önemli mülahazaları özetlemektedir. Denetçiye rehberlik sağlamak amacıyla "Alarm Sinyalleri" konusu ele alınmıştır. Alarm Sinyallerine ilave olarak; denetim meseleleri, toplanması gereken kanıtlar gibi konular ve başvuru kaynakları da bu bölümde yer almaktadır.

TANIMLAR

Kanada Hazine Kurulu Bilişim Yönetimini aşağıdaki gibi tanımlamaktadır:

"sahip olunan bilgi ve teknoloji yatırımları da dahil olmak üzere bir kurumun bilgi temelli kaynaklarının koordineli bir şekilde idaresi. Genel hedeflere ulaşabilmek, program ve hizmetleri gerçekleştirebilmek amacıyla; kurumun bilgi temelli kaynaklarının planlanması, idaresi ve kontrol edilmesi anlamına gelmektedir. Buna göre, bir kurumun sahip olduğu bilgi değerleri ve bilişim teknolojisine ilişkin olarak yaptığı yatırımlar onun değerli kaynaklarıdır ve hedeflerinin gerçekleştirilmesinde çok önemli unsurlardır." (Hazine Kurulu, Bilişim Teknolojisinin Yönetimi, Kasım 1990, syf. 5)

Kurumumuz Bilgi Teknolojisini aşağıdaki gibi açıklamakta ve tanımlamaktadır:

"Genel hedefe ulaşabilmek için kullanılan bilginin elde edilmesi, yönetimi ve dağıtılması için kullanılan destek yapısı." (6311.01, Kasım 1992)

İÇİNDEKİLER

ALARM SİNYALLERİ

EK BÖLÜMLER

BİLİŞİM TEKNOLOJİSİ ORTAMI

BİLİŞİM TEKNOLOJİSİNİN KAMUSAL ALANDAKİ ETKİSİ

1. Haziran 1993'te; iki milyarı mal ve hizmetlere bir milyarı da maaş ödemelerine olmak üzere toplam üç milyar doları aşan, bakanlık ve yönetim program gerçekleştirme maliyetlerini, yıllık iki milyar dolara indirebilmek amacıyla Bilişim Yöneticisi makamı ihdas olunmuştur. (Hazine Kurulu, *Güçlendirme*, 1993) Bu nedenle birçok Bilişim Teknolojisi destek sistemlerinin kurulması ya da mevcutların değiştirilmesi gerekmektedir.

2. Federal hükümet için görev yapan denetçiler olarak, denetlediğimiz kurumlarda gerçekleşen teknoloji değişikliklerinden haberdar olmamız gerekmektedir. Federal hükümetin bilgi teknolojisinden azami düzeyde faydalanıp faydalanmadığını anlamak için teknolojinin önünde olmamız ve kendi denetim maliyetlerimizi azaltmak için de bilişim teknolojisi denetim araçlarını kullanmaya hazır olmamız önem arzetmektedir.

GÜNÜMÜZÜN BİLİŞİM TEKNOLOJİSİ ORTAMI

3. Bilişim teknolojisi hızla gelişmektedir ve federal hükümet de maliyetlerde azalma ve verimlilik sağlayabilmek amacıyla yeni teknolojileri kullanmaktadır. Kullanıcılar, sistem sahipleri ve bilişim teknolojisi yöneticileri yeni teknolojiyi takip etmeli ve yeni teknoloji kullanımının vergi mükelleflerine hizmet sunumunu, olumlu bir şekilde etkileyip etkilemiyeceğine karar vermelidir. Bilişim teknolojisi tarafından sağlanan ve sürekli bir şekilde gelişen avantajlar, kurumların çalışma biçimini de değiştirmektedir.

- Kullanıcılar ve sistem sahipleri, verimliliğin arttırılması amacıyla sistemleri için daha fazla sorumluluk almalıdırlar. (sistem paylaşımı yada dışarıdan kaynak sağlama)

- Kurumlar maliyeti ve çalışma yükünü azaltmak amacıyla, sürekli bir şekilde hizmetlerin sunumunu değerlendirmektedirler.

- Günceli yakalayabilmek için personel eğitimi ve gelişimi çok önemlidir.

- Teknoloji sürekli olarak değiştiği için; tüm sistemin yerine oturtulmasını beklemektense, kurumun işleyen unsurlardan faydalanabilmesi amacıyla sistem gelişimi küçük gruplara bölünmelidir.

4. Bilişim teknolojisi yönetimi, hizmetlerin ulaştırılma biçimini de değiştirmektedir. Günümüzde bakanlıklar tamamiyle otomasyon sistemine geçmişlerdir. İş ihtiyaçlarını karşılayabilmek amacıyla bilgi sistemleri merkeziyetçilikten uzaklaşmaktadır. Bilişim yöneticilerini bekleyen zorluklar; bilgiyi hazır tutarken güvenlik kontrollerinin de sürdürülmesi, veri bütünlüğü ve verimliliği sağlanırken kullanıcıların sistem gelişimine katkılarının sağlanması ve hizmet ulaşım maliyetinin azaltılmasıdır.

5. "Yeniden oluşturma" ifadesi, metnin tümünde İş Sürecinin Yeniden Tasarlanması anlamında kullanılmaktadır. Yani, "maliyet, kalite, hizmet ve sürat gibi önemli ve güncel performans ölçütlerinde büyük gelişmelere ulaşabilmek amacıyla iş süreçlerinin köklü bir şekilde yeniden düşünülmesi ve radikal bir şekilde de yeniden tasarlanması" olarak tanımlanabilir (Hammer ve Champy, 1993, syf. 32). Bir çok bakanlık, teknolojinin gelişmiş bir şekilde kullanımı ile yeniden oluşturma projelerine başlamışlardır yada başlamış oldukları projeleri tam olarak sonuçlandırmak ve sonuçları rakama dökebilmek için yollar aramaktadırlar.

6. Kamusal alandaki bilginin büyük kısmı hassastır. Belirli seviyede veri gizliliği, bütünlüğü ve ulaşılabilirliğini sağlamak amacıyla politikalar üretilmiştir. Bakan yardımcıları, bakanlıklarındaki güvenlik konusunda hesap vermekle sorumlu tutulmuşlardır. Hazine Kurulu Sekreterliğinin 1987 ile 1993 yılları arasında yaptığı bir bakanlık güvenlik denetimi değerlendirmesinde, birçok bakanlığın hala Bilişim Teknolojisi Güvenliğinin yerleştirilmesinde güçlük çektiğini ortaya koymuştur (Hazine Kurulu Sekreterliği, Bilişim Teknolojisi Güvenliği Denetim Rehberi, 1994). Bakanlıklar; kabul edilebilir bir Bilişim Teknolojisi Güvenliğinin idari yapısı ve yöntemlerinin oluşturulmasında, risk yönetimi çerçevesinin sağlanmasında, muhtemel tehlikeler ve risk değerlendirmelerinin tamamlanmasında, kapsamlı ve test edilmiş olasılık planlarının geliştirilmesinde ve bilişim teknolojisinin periyodik olarak değerlendirilmesi ve denetlenmesinde sıkıntılar yaşamaktadırlar.

SÜREKLİ SİSTEM GELİŞİMİNE YENİ YAKLAŞIMLAR

7. Ciddi maddi kısıtlamalarla karşı karşıya olan birçok bakanlık, yeniden gelişimin ve yeniden tasarımın maliyetini paylaşmak üzere özel sektör veya kamu kuruluşlarından ortaklar aramaktadırlar. Hazine Kurulu Sekreterliğinde Bilişim Yöneticisinin göreve başlamasıyla, bakanlıklar arasında sistem paylaşımı konusundaki girişimler ve bakanlıkların sahip olduğu uygulama sistemlerinin sayısında muhtemel bir azalma görülecektir.

8. Başarılı program yöneticileri, Bilişim Teknolojisi projelerinin açık ve rakamlarla ifade olunabilecek yararlarını ortaya koymak suretiyle, yapacakları otomasyon teklifleri için sağlam bir temel oluşturmaktadırlar.

   Bu tür oluşumlar seçilmiş yada atanmış üst düzey yetkililerin stratejik talimatlarını desteklemektedir. Ayrıca bu durumlarda, daha küçük çaplı taahhütlerin güvenli bir şekilde yerine getirilmesi yanında, açık bir sorumluluk ve hesap verme çerçevesinin oluşturulması temeline dayanan güçlü güven ilişkileri de önem kazanmaktadır.

9. Bakanlıkların sistem değişimi ile başa çıkma yollarından biri kurumun tüm bilgi ihtiyacına aynı anda cevap verecek bir temeli oluşturacak olan "esaslı bir yapılanmanın" yerleştirilmesidir. Bu "megaprojeler" uzun yıllara yayıldığından; gecikmelere, bütçe kesintilerine, maliyet fazlalıklarına neden olabilecekleri gibi ve proje tamamlandıktan sonra da teknolojinin eskimiş olması tehlikesi ile karşı karşıya kalmaktadırlar.

BİLİŞİM TEKNOLOJİSİ DENETİMİNİN GEREĞİ

10. Bilişim yönetimi ve teknolojisini neden denetlememiz gerekir? Bunun iki önemli nedeni vardır:

- yeni uygulamaların geliştirilmesi ve eskilerin muhafazası gayretine ilaveten bilginin toplanması, işlenmesi, saklanması ve gerekli yerlere ulaştırılmasının maliyeti kamu bütçesinin giderek daha büyük bir bölümünü kapsamaktadır; bu paraların doğru bir şekilde harcandığından emin olmak durumundayız;

- kamusal işlerin yürütülebilmesi giderek artan bir şekilde elektronik teknolojiye dayanıldığından bu sistemler içinde etkili ve uygun kontrollerin yapıldığından emin olmalıyız.

11. Bilişim sistemleri ve teknolojisi; denetçinin Bilişim Teknolojisini bir model oluşturmak üzere kullanacağı durumlarda veya bir program uygulama işlevini değerlendirirken denetlenmelidir. Ayrıca bilişim teknolojisi hizmetleri; kullanıcıların, bilgi eksikliğinden yada verimsiz sistemlerden şikayetçi olduğu durumlarda da denetlenmelidir. Sistemlerin kurulmasındaki gecikmeler ve sistem geliştirme maliyetindeki fazlalıklar da proje yönetimi biriminin yada Bilişim Teknolojisi hizmetlerinin değerlendirilmesi gerektiğini belirten göstergelerdir. Sistem tamamen yerleştirildikten sonra yapılan gözlemler daha az etkili olacağı için bu bulguların sistem yerleştirilirken rapor edilmesi gerekir.

12. Bilişim Teknolojisi denetimi çerçevesi, dönüşümlü Bilişim Teknolojisi çalışması ve nadiren de takım düzeyinde daha uzmanlaşmış denetim çalışmalarının yapılmasından oluşmaktadır. Bu düzeyde uzmanlaşmış Bilişim Teknolojisi kaynaklarını elde tutmak hesaplı olmayacağı için, SFL (Sorumlu Faaliyet Lideri) kaynağı sağlayacak yada gerekli olduğu durumlarda dışarıya iş yaptıracaktır. Kurum hakkında bilgi edinmeye ilave olarak, denetim ekibi önemli görülen mali ve idari sistemlerdeki kontrol risklerini de tesbit etmelidir. Sistem kontrolüne ilişkin belgelerin kapsamlı oluşu sistemlerin önemine işaret eder. Müşteri verilerinin örnekleme yapmak üzere belirlenerek toplanması ve diğer denetim çalışmaları, takım sorumluluğunu gerektirmektedir. Müşteri dosyalarındaki verilerin yüklenmesini kolaylaştıracak yeni teknoloji sağlanıncaya kadar, denetim ekiplerine SFL yardımcı olacaktır. Yeni sistem geliştirilmesi, telekomünikasyon, bilişim güvenliği ve Bilişim Teknolojisi ünitesinin denetimi gibi uzmanlık gerektiren denetim çalışmaları, SFL'nin faaliyet alanında bulunmaktadır. SFL Bilişim Teknolojisi denetim metodolojisinden sorumlu olduğu gibi ve Profesyonel Gelişmeye ilişkin eğitim çalışmalarını da koordine etmektedir.

KURUM HAKKINDA BİLGİ

GİRİŞ

13. Kapsamlı Denetim Rehberi 6311 de belirtildiği gibi "Denetim sorumlusu, kurum ve / veya yürütülen fonksiyon tarafından kullanılan Bilişim Teknolojisinin yeterli düzeyde değerlendirilmesini sağlamalıdır". Bir kurumda bilişim teknolojisinin kullanımı belirli seviyede risk içermektedir. Bu riskin değerlendirilmesinde kullanılan yöntemler ve ilave unsurlar aşağıda belirtilmiştir. Bakanlıklar sürekli olarak yeni teknoloji kullanmaya başladıkları için; denetlenen kurumun, denetim ekibi tarafından kaydedilen bilginin güncelliğini etkileyebilecek değişiklikleri yaptığı durumlarda yeniden inceleme yapılabilmelidir.

UYGUNLUK

14. Şu anda, Hazine Kurulu Sekreterliğinin bilişim teknolojisi yönetimi konusunda biri kamusal bilgi varlığının yönetimine, diğeri ise kamu güvenliğine ilişkin olmak üzere politikaları mevcuttur. Bu politikalar, bakanlıkların bir takım girişimlere destek olmasını gerektirmektedir. Bazı politika bildirileri aşağıda kısaltılarak sunulmuştur.

Bilişim Teknolojisi Yönetimi

15. Bakanlıklar, genel koordinasyon ve hükümet talimatlarına uymalı ve Hazine Kurulu Sekreterliğinde bir bakanlık yetkilisini görevlendirmelidirler. Ayrıca bakanlıklar, araştırmalar esnasında karşılaşılacak veri hazırlama yükünden kurtulabilmek için bilişim teknolojisinden yararlanmalı ve sistemleri her iki resmi dilde de uygulamalıdırlar. Bakanlıklar, bilişim yönetimine ilişkin geniş çaplı talimatların hazırlanmasına katkıda bulunmalı ve alınan stratejik kararlara uymalıdırlar. Bakanlıklar Hazine Kurulu Sekreterliğinin bilişim teknolojisi standartlarını uygulamak ve kullanıcılardan bunların hedefleri, stratejileri ve planları hakkındaki tavsiyelerini ve izlenimlerini almalıdırlar. Bakanlıklar, plan ve hizmetlerini aynı hizmeti yapan diğer kurumlarla koordine etmelidirler.

16. Bakanlıklar işletmeci bir yaklaşımı benimsemelidirler. Bu yaklaşım, kuruma göre düzenlenmeli, kurumun önceliklerine uymalı ve program performansındaki ölçülebilir gelişmeyi göstermelidir. Sistemler arasındaki işlemlere imkan sağlayan (bakanlık içi veya dışı olabilir) ve satıcılar arasında rekabet ortamı yaratabilecek teknik stratejiler uygulanmalıdır. Bakanlıklar, en azından kendi kullanımları için, yıllık bilişim yönetim planları geliştirmeli ve 1 milyon doları geçen yeni sistemler (sermaye ve beş yıllık kullanım süresi) ve 3 milyon doları geçen eski sistemlerin değiştirilmesi için Hazine Kurulu Sekreterliğinden onay almalıdırlar. Ayrıca büyük projelerdeki maliyet artışları için de Hazine Kurulu Sekreterliğinden onay almaları gerekmektedir.

17. Kamu kurumları; çalışanları da göz önünde bulundurarak program hedeflerine ulaşmak için teknoloji kullanımının yeni yollarını bulmalıdırlar. Çalışanlar bilişim teknolojisinin icra planlarından haberdar edilmeli, onların iş güvenliği ve sağlığı için zorunlu olan uygun koşullar sağlamalı; önemli hizmetlerin sürekliğini sağlamak amacıyla test edilmiş planlar kullanılmalı ve ülke çapındaki bilgi ağının sadece kamusal işler için kullanıldığından emin olunmalıdır.

Kamusal Bilgi Varlığının Yönetimi

18. Faaliyet gereksinimlerini karşılamak ve etkin bir şekilde karar verilmesini desteklemek amacıyla, bilgi varlığının toplu bir kaynak olarak yönetimi; hükümet içinde bilginin azami düzeyde kullanımının sağlanması; kamudan gereksiz bilginin toplanmasının durdurulması ve politikalar ve program değerlendirmelerinin yeniden yapılanması veya tarihi önemi olması sebebiyle bilgi varlığının tesbiti ve muhafaza edilmesi, hükümetin politikasıdır.

Kamusal Güvenlik Politikası (KGP)

19. Kamusal güvenlik politikası Ocak 1990 tarihinde, 1994'ün başında yeniden gözden geçirilip süresi uzatılmak üzere yürürlüğe konmuştur. Bilgi güvenliği değerlendirme çalışmalarına başlamadan önce denetçilerin Sorumlu Faaliyet Liderine (SFL) danışmaları tavsiye edilmektedir. Bakanlık yetkilileri açısından KGP'nın önceliği, KGP tarafından belirlenen bir güvenlik çerçevesinin kurulması ve bu politikaya uyulduğunu gösterecek ve her beş yılda bir düzenlenecek bir iç denetim raporunu oluşturacak şekilde, periyodik değerlendirmelerde bulunulmasıdır. Denetimlerin ilk turunun Aralık 1993 tarihine kadar tamamlanmış olması gerekmektedir. Tamamlanan denetim raporlarının Hazine Kurulu Sekreterliğine gönderilmesi gerekmektedir.

BİLİŞİM TEKNOLOJİSİ HAKKINDA BİLGİ

20. Bilişim Teknolojisinin Planlamasına İlişkin Araştırma ve Denetim Kitabı (Preprinted Audit Document) 5260, denetlenen kurumun teknolojisi hakkında temel bilgileri toplamak amacıyla sık sık kullanılmaktadır. Bu araştırma, basılmış olarak ya da AUTOPADS yoluyla elektronik olarak sağlanabilir. Bilişim Teknolojisi Sorumlu Faaliyet Lideri de Bilişim Teknolojisi Araştırmasının tamamlanmasında denetçilere yardımcı olabilir. Başkanlığımızdaki otomasyon geliştikçe, bilginin güncelleştirilmesi ve bilgiye ulaşılmasının kolaylaştırılması amacıyla elektronik yolla daha fazla belgeye ulaşabileceğimizi düşünüyoruz.

21. Aşağıda bilişim teknolojisi ile ilgili risklerin değerlendirilmesinde göz önünde bulundurulması gereken önemli hususlar belirtilmektedir:

22. **Kurum ve Yönetim**

Başarılı bir Bilişim Teknolojisi Yönetimi; genel stratejiler, planlar, politikalar, metodolojiler ve standartlarla aynı çizgide bir kurumsal ortam yaratırken ve bilgisayar kullanımını ve katkısını teşvik eden bir kültür/felsefenin geliştirilmesi için çalışır. Böylelikle, kurum yetkilerinin kullanılabilmesi amacıyla, bilişim teknolojisi kaynaklarının yönlendirilmesinde üst yönetimin ve kullanıcıların katkılarını somutlaştıran bir sistemin geliştirilmesi ve muhafazasını hedef alan işletmeci bir yaklaşım benimsenmektedir.

23. Daha fazla bilgi için sıralanan yayınlara başvurulabilir: Nelms, Kontrol Hedefleri Bölüm 1, (1.1.3, 1.1.4, 1.2, 1.3) Sistem Denetlenebilirliği ve Kontrol Modül 4 Bölüm 2, SDK Modül 5 Bölüm 5.

24. **Geliştirilmekte Olan Sistemler**

Geliştirilmekte olan sistemler, hem yeni sistemleri hem de yeniden oluşturulan veya sonuçları henüz alınabilen mevcut sistemleri içermektedir. Eylül 1993'teki bir sempozyumda Başkanlığımız "Geliştirilmekte Olan Sistemler İçin En İyi Uygulama Örnekleri" konusundaki bulgularını sunmuştur. Kurumumuz, "Sihirli" çözümler üretmek yerine aşağıda özetlenen, en iyi uygulama örneklerini ortaya koymuştur. Başkanlığımızın amacı kamudaki sistem geliştirme projelerini bu " en iyi uygulama örneklerine" dayanan ölçütlere göre gözlemlemektir. Bu prensiplere ne kadar çok uyulursa risk de o derecede asgariye indirgenmiş olur. Bu tesbitlerin hiçbirine uyulmaması geliştirme projesinin başarılı bir şekilde tamamlanmasını engeller.

25. Bir sistem geliştirme projesinde; proje geciktiğinde, çalışmalar esnasında yönetim değiştiğinde, maliyetlerin birleştirilmesi zor olduğundâ ve uygulama esnasında önemli proje değişiklikleri yapıldığında sıkıntılarla karşılaşılır. Daha fazla bilgi; Bilişim Teknolojisi ile ilgili GAO Sempozyumu, Sistem Denetlenebilirliği ve Kontrol Modül 5 Bölümler 2 ve 4, ve halen Grup 8 tarafından hazırlanmakta olan "Geliştirilmekte olan Sistemler için Sayıştay Denetim Metodolojisi ve Kriterleri" isimli belgelerden sağlanabilir.

26. İşletmeci yaklaşımında ; yeni ve eski sistemlerin maliyet, fayda ve risklerine dayanan öncelikler belirlenmelidir. İhtiyaç duyulduğunda kaynak hazır olmalıdır.

27. Projenin dayanağı ortak genel strateji olmalı, işin önemli fonksiyonları desteklenmeli ve kullanıcılarda bir "sahiplenme" duygusu ve projeye bağlılık yaratacak şekilde *kullanıcı ihtiyaçları tarafından yönlendirilme anlayışı yaratılmalıdır.*

28. Projeler seçildikten sonra üst yönetim tarafından sahiplenilmelidir.

29. Sistem geliştirme sürecinin ilk aşamalarındaki etkin bir proje yönetimi ileride çıkabilecek muhtemel güçlükleri azaltır. Proje için kısa ve ölçülebilir bir zaman çerçevesi oluşturularak gerçekleştirilmesi kolay küçük ama kendine yeten bölümler yaratılmalıdır.

30. Farklılık lider ve ekip üyeleri tarafından oluşturulur. Proje yöneticilerinde karar alabilecek yetki ve cesaret bulunmalıdır. Ekip sonuç yönelimli ve iş bitirici olmalıdır. Ekibin sürekliliği, özellikle uzun vadeli projelerde çok önemlidir.

31. Geliştirme ekibi ve kullanıcılar arasında, sistem gelişimi konusunda iletişim sağlanması çok önemlidir; kullanıcılar, gelişmelerin işleri üzerindeki etkisi ve eğitim ihtiyaçları konularında bilgilendirilmeyi beklerler.

32. Okuyucular ayrıca Kontrol Hedefleri Bölüm 1 (2.2 - 2.7), Auerbach 74 - 04 - 50 den ve geliştirilmekte olan sistem kriterlerinden faydalanabilirler.

33. **Sistem Kontrolleri**. Denetçilerin yıllık olarak, yönetimin verdiği işlem yetkilerini, varlıkların korunması ve mali bilginin güvenirliği ile ilgili işlemleri değerlendirmeleri gerekir. Daha fazla bilgi şu kitapçıklardan sağlanabilir: Kontrol Hedefleri Bölüm 1 (4.1 - 4.4), Sistem Denetlenebilirliği ve Kontrol Modül 2 Bölüm 3, SDK Modül 5 Bölüm 5 ve SDK Modül 6 Bölüm 1.

34. **Kullanılan Teknolojiye İlişkin Risk.** Bir kurum tarafından seçilen teknolojinin türü ve kurumun bu teknolojiyi başarılı bir şekilde uygulayabilme kapasitesinin risk / başarı unsurları üzerinde çok büyük etkisi vardır. Örneğin:

- **İşleme**. Tek başına işlemeden başlayarak, yerel bilgi ağı kümelerine ve daha sonra da ana bilgisayarlarla kişisel bilgisayarı birbirine bağlayan teşebbüs çapındaki oluşumlara aktarım giderek zorlaşmaktadır. Benzer şekilde toplu işleme ortamından, bölümlere ayrılan işleme ortamına veya telekomünikasyondan aşırı derecede yararlanan işleme ortamına geçmek de giderek daha zorlaşmaktadır. Mevcut standart teknolojinin alınması, uyarlanması ve muhafazası, genellikle özel olarak toparlanıp bir araya getirilmesinden daha kolaydır.

- **Kullanıcılar**. Kullanıcıların, az yada hiç merkezi yönlendirme olmaksızın bilgisayar kullanımının büyük bir kısmından sorumlu oldukları durumlarda gelişme üzerinde bir kontrol eksikliği oluşabileceği gibi, bilginin güvenilirliğini sağlayamayan sistemlere haklı bir nedene dayanmaksızın bir güven duyulması ile karşılaşılabilir. Denetçilerin, denetledikleri kurumdaki mevcut durum hakkında bilgi sahibi olmaları ve bu sistemlerin güvenilir olduğunu kabul etmeleri halinde, uyguladıkları yaklaşımı belgelendirmeleri ve muhtemel riskleri belirlemeleri gerekir. Denetçilerin, kişisel bilgisayarlarda ve yerel bölgelerdeki bilgi ağlarında kullanılan yazılımın yasal korunum politikalarını ve standartlarını da bilmeleri gerekmektedir. Ayrıca, denetledikleri kurumun virüs bulaşmamış bir yazılım ortamını sürdürebilmek için uyguladığı yöntemleri de bilmeleri gerekmektedir.

35. Daha fazla bilgi için: Auerbach 72-03-10, 75-01-50'den 60.1'e kadar, SDK Modül 7 Bölüm 2, 3, 4 ve KH Bölüm 2 (5.1-5.5).

36 **İnsan Kaynağının Bilişim Teknolojisinin Uygulanabilmesi Amacıyla Kullanımı.** Bilişim teknolojisi ortamındaki kişiler, denetlenen aynı kurum içinde bile, kişiden kişiye değişen jargonlar geliştirmişler ve kullanmaktadırlar. Bu, sistemi belgelendirmek isteyen denetçiler için zorluk çıkartabilir. Bir diğer zorluk da Bilişim Teknolojisi uzmanlarının yeterli düzeyde eğitilip eğitilmedikleri ve iyi yönetilip yönetilmediklerinin belirlenmesidir.

37. Bazı Bilişim Teknolojisi uzmanlarının sisteme doğrudan giriş hakları vardır ve böylece kontrollerin tümünü aşabilirler. Buradaki zorluk, bu kişilerin kurumun tam güvenine sahip olmaları halinde sistem bütünlüğüne bir tehdit oluşturup oluşturmadıklarının anlaşılmasıdır.

38. Kurumlar yapılması gereken iş için gerekli yeteneklere sahip kişileri seçmeye gayret göstermelidirler. Hem kullanıcılar hem de bilişim teknolojisi personeli yeterli derecede eğitimden geçirilmeli ve gelişmeleri sağlanmalıdır. Sürekli personel yerine sözleşmeli yada geçici personel kullanılması, sürekliliğin ve ortak bilgi düzeyinin sağlanamaması risklerini taşımaktadır.

39. **Faaliyetler**. Faaliyetler, genellikle yüksek risk taşıyan alanlar olarak görülmektedirler. Bu yargı, fiziki değerlerin korumasında geçerli olsa bile bilgi ele alındığında geçerliliğini yitirmektedir. Büyük faaliyetlerin verimliliğinin değerlendirilmesi için çok fazla çalışma ve inceleme yapılmıştır. Denetçiler, denetledikleri kurumundaki verileri ülkedeki diğer bilgi merkezleri ile kıyaslamak amacıyla araştırma şirketlerinin hizmetlerinden güvenle yararlanabilirler. Faaliyetlerdeki risk alanları aşağıdaki gibidir:

- Acil iletişim, kısa süreli araştırma ve rapor hazırlama ve mikro - bilgisayar desteği gibi kullanıcı destek faaliyetleri yoksa zamanın ve kalitenin çok önemli olduğu büyük sistemlerde, kullanıcılarla yapılan servis anlaşmaları sistemin risklerini ve zayıflıklarını ortaya çıkarabilir.

- Veri merkezleri fiziksel zararlara ve yetkisiz kişilerin bilgiye ulaşmasına karşı korunmalıdır. Büyük bilgi merkezlerinde genellikle kullanıcıların çevirmeli modem ile bilgiye ulaşabilme imkanı mevcuttur. Ancak bu sistem yetkisiz girişlere de olanak sağlayabilmektedir. Merkezlerde cihazlara yetkisiz girişleri tesbit edecek ve önleyecek özel donanım ve yöntemlerin bulunması gerekmektedir.

- Yangın, sel, zelzele ve çalışanlar arasındaki huzursuzluğun faaliyetler üzerinde etkisi vardır. Önemli uygulamalar için kurumda beklenmedik olaylara ve felaketlere karşı test edilmiş önlem planları bulunmalıdır. Donanım ve faaliyet yazılımları için destek ve geri kazanım yöntemleri, faaliyet yazılımları ve uygulama programlarının da mevcut olması gerekmektedir.

40. Daha fazla bilgi için: KH Bölüm I (3.1 - 3.3) ve SDK Modül 4 Bölüm 3.

GÜVENLİK VE DESTEK SÜREÇLERİ

41. Hayati önem taşıyan tüm dosyalar ve programlar desteklenmeli (kopyaları hazırlanarak) ve ilgili belgeler, el kitapları ve formlarla birlikte başka bir yerde saklanmalıdır. Desteklemenin ne kadar sıklıkla yapılacağı sistemin ne kadar önemli olmasına bağlıdır. Bu, online sistemlerinde hemen yapılabilirken daha az önem taşıyan uygulamalarda saat başı yada haftalık olarak gerçekleştirilebilir. Bu "hafif" desteklemelere ilave olarak, uzun vadeli donanım hatalarında işleme derhal başlayabilme imkanı da olmalıdır. Beklenmedik olay veya işe yeniden başlama planlarına, benzer makinalara giriş veya bakım anlaşmaları da dahil edilmelidir. Dolayısıyla denetçi işlemekte olan süreçleri anlayabilmek için yukarıda belirtilen hususların mevcudiyetini ve test edilme sıklıklarını saptamak zorundadır.

42. Daha fazla rehberlik için: KH Bölüm 1 (3.4 - 3.5), Auerbach 73-01-50, 75-02-20, 75-02-40, SDK Modül 10 Bölümler 2, 3, 7, ve 8.

TELEKOMÜNİKASYON

43. Telekomünikasyon teknolojisi insanların ve makinaların uzun mesafelerden iletişim kurabilmelerini sağlamaktadır. Bölümlere ayrılan işleme, değişik işlem seviyelerindeki yazılım programlarının veriyi etkilediği durumlarda gerçekleşmektedir. Tipik bir işlem; bilginin yerel ofislerde toplanıp derlenmesi, daha sonra bölge ofisindekilerle birleştirilip bir daha derlenmesi ve son olarak da merkezi tesise " boşaltılmasıdır". Her kademe bir önceki kontrollerden faydalanır ve her kademenin yapılan işlemde payı vardır. Bu kademelerde yapılan incelemelerde eldeki verinin bütünlüğünden yararlanılır. Buna; merkezi bilgisayar ile yerel ve genel olan bilgi ağları ve taşıyıcı şirket tarafından sağlanan ortak tesisler de dahildir.

44. Yerel bilgi ağlarının artan bir şekilde kullanılması, mini işlem alanlarının gelişmesine ve kullanıcılar ile merkezi alanlar arasında bir işlem köprüsü vazifesi görmesine yol açmıştır. Böyle bir durum sözkonusu ise yüksek seviyelere geçirilmeden önce, daha düşük seviyelerde birçok işlemin yapıldığı bir işbirliğinin sözkonusu olduğu düşünülebilir. Kurumu anlamak, bu tür faaliyetler ve ortaklaşa işlemden faydalanan sistemler hakkında bilgi sahibi olmak anlamına gelmektedir. Hatalar ve atlamalar riskin önemli bir kısmını oluşturmaktadır ve veri elde edilmesi anında gerçekleşmektedirler.

45. Bilgi ağında gerekli olan özel kontroller, bilgi ağının desteklediği uygulamaların ve bilgi ağını kullanan kurumun türüne göre değişmektedir. Uygulama risklerine; gizli bilgiye yetkisiz giriş, bilginin kötü amaçlarla kullanılması, iş faaliyetlerinin aksatılması ve yanlış veya tamamlanmamış bilginin sisteme sokulması dahildir. Önemli başka bir unsur da bilgi ağının verimli ve tutumlu bir şekilde yönetimi ve aktarılan bilginin kontrolüdür.

46. Daha fazla bilgi için: Bilgi İşlem Denetimi Dergisi, "Bilgi İletişimi Denetim Sorunları", Cilt III., 1989 syf. 37 ve Bilgi İşlem Denetimi Dergisi "PBX Güvenliği", Cilt II 1993, syf. 37, CO Bölüm II (2.1-2.5, 5.1-5.5, 6.1-6.2), SAC Modül 8 Bölümler 2, 5, 7 ve 8, ve Auerbach 74-01-60.1.

BİLİŞİM TEKNOLOJİSİNDE MALİYET DEĞERLENDİRMELERİ

47. Bu değerlendirme ile yönetimin Bilişim Teknolojisine ne kadar para harcandığını bilip bilmediği saptanmalıdır. Bilgi İşlem Dergisinde de belirtildiği üzere, "Yönetim toplam Bilişim Teknolojisi maliyetini ve bunun nelerden oluşduğunu bilmelidir. Genellikle, yönetim, Bilişim Teknolojisi bölüm maliyetinin tüm Bilişim Teknolojisi maliyetini temsil ettiğini düşünür. Ekipmanın eskimesi, sistem geliştirme projeleri üzerinde kullanıcılar tarafından harcanan vakit, kullanıcı alanlarındaki Bilişim Teknolojisi destek personeli ve kullanıcı bütçelerine dahil olan Bilişim Teknolojisi projelerinin hepsi birer gizli Bilişim Teknolojisi maliyet kalemidir." (Nelms, C., Bilgi İşlem Denetimi Dergisi, Cilt III 1992)

48. Denetçiler yönetimin bilişim teknolojisi hizmetlerinin toplam maliyetinin hesabını verip veremediklerini tesbit edeceklerdir. Bunların içinde; faaliyetlerin, sistem geliştirmelerinin, telekomünikasyonun, kullanıcıların ve bilişim teknolojisi personelinin eğitiminin, sistem hatalarının düzeltilmesinin, donanım kiralamalarının, yazılım destek anlaşmalarının, kişisel bilgisayar destek faaliyetlerinin, veri güvenliğinin ve bilişim teknolojisi yönetim desteğinin maliyetleri bulunacaktır.

49. İdeal olarak, yukarıda belirtilen maliyetler kuruma sağlanan hizmetlerle kıyaslanarak değerlendirilmeli ve bilişim teknolojilerinin kurum için hesaplılığını belirlemek için de diğer kurumlardan alınan rakamlarla karşılaştırmalar yapılmalıdır. Bu soruların cevapları hangi sistemin veya bilişim teknolojisi kaynağının alınacağına ilişkin kararların da temelini oluşturacaktır. Gerçekçi maliyetlere sahip olmadan yeni sistem geliştirme tahminlerinin doğru yapılması ve bunların savunulmasını olanaksızdır.

50. Daha fazla bilgi SDK Modül Bölümler 2 ve 3'de mevcuttur.

BİLİŞİM TEKNOLOJİSİ VE PERFORMANS DEĞERLENDİRMELERİ

GİRİŞ

51. Bilişim teknolojisinde iyi bir performans elde edebilmek için, kurumlar genel hedeflere ulaşmak, program ve hizmetleri gerçekleştirebilmek amacıyla kurumun bilgi temelli kaynaklarını planlamalı, yönetmeli ve kontrol etmelidirler.

52. Bilişim teknolojisi politikalarının yönetimi konusunda; Hazine Kurulu Sekreterliği "hükümetin bilişim teknolojisi yönetimindeki amaç; bu teknolojinin, kamusal öncelikleri ve programa dayalı faaliyetleri desteklemek, üretkenliği arttırmak ve kamu hizmetinin daha iyi hale getirilmesini sağlamak amacıyla kullanılmasını temin etmektir" demiştir.

53. Genellikle, bilişim teknolojisinin performans denetimi, daha geniş kapsamlı bir program denetiminin bir unsuru olarak gerçekleştirilmektedir. Dolayısıyla denetçiler, denetlenen programı destekleyen sistemleri gözden geçirmeli ve bilişim teknolojisi unsurunda, tutumluluk, verimlilik ve etkinliğin gerçekleşip gerçekleşmediğini belirlemelidirler. Bu teknoloji ve uygulamasının daha da karmaşık bir hal aldığı durumlarda, bilişim teknolojisi denetçilerinin, kurumun bilişim teknolojisi bölümlerini denetlemeleri ve bakanlık tarafından izlenen bilişim teknolojisi planlarını, hedeflerini ve stratejilerini değerlendirebilmek için daha fazla zaman harcamaları gerekmektedir.

54. Bilişim teknolojisi Sorumlu Faaliyet Lideri, Mikrobilgisayar Çalışması (Bölüm 15, 1987), Bilgi Güvenliği Denetimi (Bölüm 9, 1990) ve Geliştirilmekte Olan Sistemler Sempozyumu (Eylül 1993) gibi geniş çaplı çalışmalarını sürdürmeye devam edecektir.

BİLİŞİM TEKNOLOJİSİNDE PERFORMANS

55. "Bilişim teknolojisinde performansın iyi olması; kurumun amaç ve stratejilerinin net bir biçimde tesbit edildiği; bilişim teknolojisi kaynaklarının mal ve hizmet üretiminde en fazla karşılık alınacak şekilde tahsis edildiği anlamına gelmektedir. Ayrıca, genel stratejiye ulaşmak üzere yapılan faaliyetler için hangi sistemler, altyapılar ve nitelikler gerektiğini belirten bir bilişim stratejisi de mevcut olmalıdır" (Nelms, 1992).

56. Öncelikler belirlendikten sonra, bilişim teknolojisi denetçisi aşağıdaki hususların gerçekleştiğinden emin olmalıdır:

- **Etkinlik**. Bilişim teknolojisi denetçisi, bu teknolojiye harcanan paranın kurumu önceden belirlenen hedeflerine yaklaştırdığından (doğru işlerin yapıldığından) emin olmak isteyecektir.

Verimlilik Bilişim teknolojisi denetçisi kurumun satın aldığı bilişim teknolojisi kaynaklarından azami suretle faydalanıp faydalanmadığını bilmek isteyecektir.

- **Tutumluluk**. Bilişim teknolojisi denetçileri satın alınan teçhizat ve hizmetlerin kurumun belirlenen ihtiyaçlarını karşılayıp karşılamadığını ve uygun bir fiyatla alınıp alınmadıklarını belirlemek zorundadırlar.

57. Bilişim teknolojisindeki tutumluluk, verimlilik ve etkinliğin belirlenmesi ve bu teknolojinin başarılı bir şekilde kullanılıp kullanılmadığının anlaşılması için iki yaklaşım uygulanmaktadır. İlk yaklaşım, bilişim teknolojisi bölümünün tüm işlevlerinin sadece incelenmekte olan program çerçevesinde değerlendirilmesidir. Bu yaklaşım, devam etmekte olan program denetiminde yararlanılacak hızlı ve faydalı sonuçlar ortaya çıkarmak suretiyle kurum hakkında ek bilgiler sunar ve kurumdaki bilişim teknolojisinin durumu hakkında genel bir bilgi edinilmesini sağlar.

58. İkinci yaklaşım, bilişim teknolojisi işlevinin gözden geçirilmesi ve kullanıcıların ihtiyaçlarının karşılanmasını sağlamak amacıyla etkinliğinin, verimliliğinin ve tutumluluğun değerlendirilmesidir. Bu yaklaşım başarılı olmuş ve özel incelemeler esnasında kullanılması kurumlar tarafından takdirle karşılanmıştır. İlk yaklaşım, bir bilişim teknolojisi Sorumlu Faaliyet Lideri rehberliğindeki denetim elemanları tarafından gerçekleştirilebildiği halde ikincisinin uygulanışı tamamen bilişim teknolojisi Sorumlu Faaliyet Liderinin özel çalışma alanına girmektedir.

BİLİŞİM TEKNOLOJİSİNDE PERFORMANS DENETİMİ - BİR PROGRAM DEĞERLENDİRME UNSURU

59. Bundan sonraki bölümlerde; geçmişte iyi neticeler alınan ve denetim için harcanan zamanın karşılığının bulunduğu birinci yaklaşım üzerine yoğunlaşacağız. Genel inceleme ve ön hazırlık çalışması esnasında saptanan sorunlar ve riskler, aşağıda belirtilen incelemelerden hangilerinin ve ne dereceye kadar yapılacaklarını belirleyecektir. Bilişim teknolojisi denetimini daha ayrıntılı bir biçimde gerçekleştirmek isteyenler bilişim teknolojisi SFL ile temasa geçmelidirler.

60. **Bilişim Teknolojisi Plan ve Stratejileri**. Kurum veya Kuruluşun stratejisi ile bilişim teknolojisi stratejisi birbirine bağımlıdır. Bilişim teknolojisi stratejileri, insan kaynağı ve finansman stratejilerinin yaptığı gibi, iş planlarını desteklerler. Bilişim teknolojisi, kurumun hedeflerine daha etkin bir şekilde ulaşmasının bir aracı olduğu gibi bütünleşik planın da bir parçası olmalıdır. Kamu kurumlarındaki bilişim teknolojisi plan ve stratejileri, Hazine Kurulu Sekreterliği tarafından belirlenen şekilde Bilişim Yönetimi Planları kapsamına alınmalıdır. Zamanlılık, doğruluk, güvenilirlik ve kuruma özgü olmak gibi özelliklerin tümü, kurumlara stratejik bir avantaj ve maliyetlerde düşüş sağlayabilecek bilgi nitelikleridir ve bunların bilişim teknolojisi stratejilerine dahil edilmeleri gerekir.

61. Denetçiler öncelikle, kurumun genel stratejisinin kapsamını araştırmak ve bunun incelenmekte olan programın bir bölümü olarak bu stratejiyi destekleyip desteklemediğini saptamak zorundadırlar. Ayrıca, kullanılmakta olan sistemlerin program stratejisinin bir bölümünü oluşturup oluşturmadığından ve eğer oluşturuyorlarsa bunun ne şekilde gerçekleştiğinden emin olmalıdır. Performans denetçileri; programın uygulanışında ulaşılan bilişim teknolojisi düzeyinin, bu teknoloji kullanılmaya başlanıldığında umulan faydaları (verimlilik, üretkenlik ve kalite artışları) sağlayıp sağlamadığıyla da ilgileneceklerdir.

62. **Sistemlerin Uygunluğu**. Bir performans değerlendirmesinde, kullanıcıların programı destekleyen bilişim teknolojilerinin verimliliği hakkındaki görüşleri çok önemlidir ve hemen hemen değerlendirmenin tüm alanları hakkında değerli bilgiler sağlamaktadır. Bilişim teknolojisinin performans denetimi esnasında ulaşılan sonuçların birçoğu denetçinin yargısına dayanmaktadır ve bu sonuçların kullanıcıların görüşleri ile doğrulanması çok faydalı olacaktır. Denetçi; kullanıcıların, programın gerçekleştirilmesinde kullanılan sistem hakkındaki görüşlerini ve değerlendirmelerini elde etmek amacıyla anketler ve diğer bilgi toplama tekniklerini kullanmayı düşünmelidir.

63. Denetçi, sistem uygulamasının geliştirilmesi aşamasında kullanıcılara danışılıp danışılmadığını; bilişim teknolojisi organizasyonunun kullanıcı tatminini nasıl tesbit ettiğini ve bunu planlarına nasıl yansıttığını; planların uygulanışının ve sonuçlara ulaşımın nasıl ölçüldüğünü bilmek isteyecektir. Denetçi için; kurumun, mevcut teknolojiden sistemin uygulanışının kolaylaştırılması amacıyla istifade edip etmediğinin ve bilişim sistemlerini geliştirmek ve iyileştirmek amacıyla hazırlanarak onaylanmış bir yaşam dönemi çevrimi metodolojisinin (life cycle) takip edilip edilmediğini tesbit etmek de önemlidir.

64. **İnsan Kaynağı** Bilişim teknolojisi hizmetlerinin yerine getirilebilmesi için, gereken becerilere gereken zamanda sahip olunması ve bunlardan yararlanılması hayati önem taşımaktadır. Yönetim, bilişim teknolojisindeki gelişmeleri takip etmeli ve bunların mevcut faaliyetlerden en çok hangilerini etkileyebileceğini tesbit etmelidir. Yönetim, programın uygulanışında kullanılan sistem hakkında bilgi sahibi olan ve gelecekteki gelişmeler için de alternatif senaryolar yaratabilen personel çeşitliliğine sahip olmalıdır. Kurum, bu hususları göz önünde tutarak sistemin uygulanışında görevli olan tüm personel için bir eğitim planı geliştirmelidir.

65. Denetçi; Kurumun, sistemin sürekli olarak geliştirilmesinden sorumlu olan personele uygun eğitimi (hizmet içi eğitim, konfernslar, ürün sunuşları ve seminerler) sağlayıp sağlamadığını öğrenmek isteyecektir. Eğitim sadece teknolojik konularda değil, üretkenliğin geliştirilmesi, hizmetin kalitesi ve destek hizmetleri ile de ilgili olmalıdır.

66. **Bilişim Teknolojisi Hizmetlerinin Yerine Getirilişi.** Yönetim, programın uygulanışını kolaylaştırmak amacıyla, bilişim teknolojisi hizmetlerini izlemek ve değerlendirebilmek üzere birtakım olanaklara sahip olmalıdır. İdeal olarak; yönetim, programdaki toplam bilişim teknolojisi maliyetlerini bilmeli ve programın iyi bir şekilde uygulanıp uygulanmadığını izlemek amacıyla verimliliği ölçmelidir. Bu ölçüme; araştırılan bir konuya bilgisayarın cevap verme süresi, belirli bir zaman sürecinde yapılan işlem sayısı ve hataların türü veya alınan şikayetlerin sayısı dahil edilebilir. Kritik ölçümlemeler, bilişim teknolojisi fonksiyonu ile yapılmış olan hizmet sözleşmesinin bir parçası olmalı ve program yöneticileri tarafından gözlenmelidir.

67. Denetçi; yönetimin, bilişim teknolojisi maliyetlerini verimli bir şekilde izlenmesi, kaynakların tahsisi ve hizmetlerin yürütülmesi konularında elindeki bilgileri nasıl kullandığını öğrenmelidir. Denetçinin; kullanıcıların (müşterilerin) bilişim hizmetlerinin etkin bir şekilde yürütülüp yürütülmediğini nasıl ölçtüklerini saptayarak, bulgularını program yöneticilerinin planları ve bilişim teknolojisi fonksiyonu planları ile mukayese etmesi gerekmektedir.

68. **İş Akımının Yeniden Tasarlanması için Olanaklar**. Denetçi, teknoloji yatırımlarının programın yürütülmesini destekleyecek kapasiteye ve esnekliğe sahip olduğundan emin olmalıdır. Sistemlerin daha etkin bir şekilde işleyip işleyemeyeceğinin; mevcut teknolojiden azami bir şekilde yararlanılması suretiyle prosedür ve işlemlerde yapılabilecek değişikliklerin hizmet kalitesini, kullanıcıların tatminini ve genel olarak üretkenliği arttırıp arttıramayacağının değerlendirmesi de denetçinin görevleri arasında bulunmaktadır.

69. Kullanılan teknolojinin hala uygun olup olmadığını belirlemek amacıyla denetçi bölümlere ayrılan işleme, telekomünikasyon ve bilgi güvenliği gibi konuları da değerlendirmelidir. Çoğu durumda; sistem kullanıcılarının yorumlarının dikkatli bir şekilde incelenmesi, denetçiye sistemin gelecekte alacağı yönü gösterecek önemli ipuçları sağlayacaktır.

70. **Bilişim Teknolojisinin Maliyeti**. Bilişim teknolojisinin maliyetinin tesbitine ilişkin çalışma; denetçinin, yönetimin aynı bilgiye başka yöntemlerle nasıl ulaşılabileceği ve bu bilgi olmadan çalişmalarını sürdürüp sürdüremeyeceği konularında fikir edinebilmesini sağlar. Performans incelemelerinde, karşılaştırma yapmaya elverecek şekilde benzer büyüklükte, karmaşıklıkta ve aynı yetkilere haiz kurumların bulunması güçlüğü vardır. "Aynı alandaki rakipler"in sayısı pek fazla değildir.

71. Faaliyetler ve bilgi merkezleri için maliyet bilgisinin elde edilmesi daha kolaydır. Çünkü temel çalışmalar ve uzmanlar mevcuttur. Diğer alanlarda ve benzer kurumlarla bu gibi araştırma çalışmalarının yapılmasına karar verilirken dikkatli olmak gerekir. Bilişim teknolojisi SFL maliyet belirlenmesi, geçerliliği ve değerlendirilmesi gibi konularında zorluklarla karşılaşan denetçilere yardımcı olabilir.

EK REHBERLİK

72. Aşağıda belirtilen alanlardaki çalışmaların da performans denetimlerinde faydalı olduğu belirlenmiştir.

73. **Bilişim Güvenliği**. Denetçi programı destekleyen uygulama sisteminin çevre ve giriş kontrollerini inceler. Denetçi, sistemin güvenliğinin iç denetim tarafından ne zaman denetlendiğini ve güvenlik kontrollerinin başka bir kuruluş tarafından değerlendirip değerlendirmediğini öğrenmelidir. Sisteme giriş kontrollerinin (kullanıcı kimlik tesbiti, şifreler, modemler vasıtasıyla dışarıdan giriş) yeterliliği denetçi tarafından değerlendirilmelidir.

74. Denetçi kullanıcıların giriş şekillerini gözden geçirmeli ve bunların görevleriyle çelişip çelişmediğini belirlemelidir. Denetçi, destek ve geri kazanım yöntemlerinin uygun olduğundan ve bunların işin yeniden başlatılması planında yer aldığından emin olmalıdır. Denetçi bu yöntemlerin test edilip edilmediğini saptamalıdır.

75. **Telekomünikasyon**. Bazı kurumlar bilişim teknolojisi için bütçelerinin üçte birini ayırdıkları halde, telekomünikasyona gereken önem verilmemektedir. Denetçi kullanılan bilgi ağı ve hizmetlerin nasıl verildiği konusunda bilgi edinmelidir. Yapılabilecek hızlı bir testle; aylık faturalarla, kurulu sistem kıyaslanabilir. Denetçi aylık faturadan yararlanarak, kullanılmadığı halde parası ödenen hizmetleri de tesbit edebilir.

76. Denetçi; kullanıcıların bilgi ağının bakımı için sunulan hizmetlerden memnun olup olmadıklarını öğrenmeli ve bilgi ağının kullanılabilirliğini de değerlendirmelidir. Bölgelerdeki federal kuruluşların, hizmetleri ve destek tesislerini birbirleri ile paylaşmaları teşvik olunmalıdır. Denetçi, denetlenen kurumun aynı bina içindeki diğer kamu kuruluşları ile iletişim tesislerini paylaşmak hususunda girişimde bulunup bulunmadığını da belirlemelidir.

TASDİK DENETİMİNE İLİŞKİN KONULAR

GİRİŞ

77 Tasdik denetimi yapılırken, önemli iç kontrollar ve kontrol ortamı hakkında bilgi edinilmesi kaçınılmazdır. Belgelendirmeye ilişkin standartlar kesin olup, denetimin boyutlarına göre farklılık gösterebilir. Denetçi iç kontrollara güvenip güvenmeyeceğine karar vermelidir. Eğer bunları güvenilir bulursa, sözkonusu kontrolların bütünlük, doğruluk ve geçerlilik açılarından teste uygun olup olmadığını da tesbit etmelidir.

SİSTEM KONTROLLARI

78. Veri girişi, işlemesi ve çıkışına ilişkin olarak yapılacak anahtar uygulama kontrolları; işlemlerin tümünün eksiksiz ve doğru bir biçimde ve zamanında yapılmış olması nedeniyle onaylanarak kaydedildiği hususunda güvence sağlayabilmelidir. Testler denetime alınan dönemin tamamını içine alacak şekilde yürütülmelidir.

79. Uygulama kontrolları; kullanıcı yöntemleri (girdi ve çıktıların kişiler tarafından ayarlanması) veya programlanmış otomasyon yöntemleri (işlemlerde, belirlenen bir asgari dolar seviyesinin aşılmamasının sağlanması) şeklinde olabilir. Otomasyon kontrol yöntemleri, ortamın uygunluğuna ve genel bilgi sistemleri kontrollarına son derecede bağımlıdır ve bunlar olmaksızın sisteme güvenilmesi doğru olmayabilir.

80. Uygulama kontrolları sistem içindeki kontrolların, doğru ve usulüne uygun olduğu hususunda güven verebilecek şekilde tasarlanmalıdır. Ayrıca kaydedilen işlemler üzerinde; verilerin doğru olduğunu ve sahtecilik ihtimalinin en az seviyede olabileceğini güvence altına alabilecek kontrollar da yapılmalıdır.

81. Kontrollar kişiler tarafından veya otomasyon yöntemleriyle veya her ikisini de kullanarak gerçekleştirilebilir. Birden fazla kontrol hedefini karşılamak amacıyla birden fazla prosedür tasarlanmalıdır. Hangi kontrol yöntemlerine güvenileceği denetçiye kalmıştır. Denetim verimliliği, kontrollara ne derecede güvenileceğine karar verilmeden önce gözönünde bulundurulacak bir husustur.

82. Daha fazla bilgi için SDK Modül 2 Bölüm 1 ve 3 ve Auerbach 72-03-60.

BİLGİSAYARIN KİŞİLERCE KULLANIMI VE BÖLÜMLERE AYRILAN İŞLEMLER

83. Birçok kurumda bilgisayarın kullanımında, katı kuralların olmadığı bir ortam veya yok denilecek kadar az kısıtlama söz konusudur. Daha kısa zamanda bilgi elde edilebilmesi amacıyla geleneksel bilişim sistemi usulleri göz ardı edilebilmektedir. Resmi değerlendirme yöntemleri mevcut olmayabilir ve kullanıcılar sonuçların doğruluğunu

onaylayacak kaynaklara sahip bulunmayabilirler. Genellikle kullanıcı tarafından yaratılan bilgiler çok az kontrol edilmektedir.

84. Uygulama programları üzerinde çok az test yapılabilir ya da hiç test uygulanmayabilir. Kopyalama ve geri kazanım yöntemleri genellikle yetersizdir ya da mevcut değildir. Mikrobilgisayarlar, programlar ve veri üzerindeki güvenlik önlemleri yok denecek kadar az olabilir. Bu durum usulüne aykırı değişikliklere, yazılıma virüs girmesine yada verinin yok olmasına neden olsa da kullanıcıların bilgisayara alışmalarına ve bilgisayar ile ilgili bilgilerinin artmasında yararlı olacaktır. Bu genellikle olumlu olarak değerlendirilmekteyse de denetçinin, kullanıcının bilgiyi kağıda dökme aşamasında gereken tüm önlemleri almadığı durumlarda bu bilgilere güvenilemeyebileceğinin bilincinde olması gerekmektedir.

85. Genellikle, sürekliliği sağlayacak belgeleme azdır yada hiç belgeleme bulunmamaktadır. Kullanıcı tarafından yaratılan uygulama yazılımı; programların esnek olmaması ve öğrenilmelerinin zor olması veya verilen bir görev için fazla spesifik olması nedenleriyle, genellikle tasarımcının veya programcının onayını alamamaktadır. Dolayısıyla boşu boşuna gayret sarfedilmiştir.

86. Bu sistemler risk bakımından değerlendirilmelidir. Bu değerlendirmede aynı denetim standartları uygulanır ama riskin değerlendirilmesi, yapılan işlemlerin önemine göre olacaktır. Denetçiler, eğer bunlara itibar edeceklerse; kullanıcı sistemlerinin girdi, işleme ve çıktı kontrollerini belgelemeli ve test etmelidirler.

87. Daha fazla bilgi için: SDK Modül 7 Bölüm 3 ve 5, ve KH Bölüm II (5.1-5.5).

88. Bölümlere ayrılan işleme, kontrollerin de bölümlere ayrılmış olduğu anlamına gelmektedir. Bu durum kurumların riskini arttırmaktadır. Risklerin bir kısmı tecrübesiz veya eğitimsiz personelden kaynaklanmaktadır. Bu hal; kullanıcıların, normalinde onların da bildiği giriş güvenliği, destek/geri kazanım (kopyalama) ve program değişikliği gibi konularda sürdürdükleri kontrollara güvenilmesini güçleştirmektedir.

89. Tecrübeli bilgisayar kullanıcıları, gerektiğinde başvurulabilecek ancak büyük ihtimalle kaynağı şüpheli ve tam olarak doğru olmayan bilgilerin yer aldığı "kara kitap" sistemlerinden yararlanmaktadırlar. Eğer denetçi bu sistemlere itibar edecekse, kontrolları test etmelidir. Aynı şekilde, belki de daha önemlisi, denetçi "resmi" sistemler varken neden kara kitap sisteminin kullanıldığını da araştırmalıdır. Bu inceleme sonucunda, mevcut sistemdeki kusurlar tesbit edilerek sürecin yeniden tasarlanması gereği vurgulanabilir.

90. Bölgesel bilgisayar siteleri olan kurumlarda faaliyet programlarının dağıtımı; her birimin aynı programı uyum içinde ve istikrarlı bir şekilde kullanmasını sağlayacak şekilde merkez tarafından yürütülmektedir. Tüm siteler kabul edilen aynı uyarlamayı kullanmalıdırlar. Ayrıca, yetkisiz değişikleri asgariye indirmek amacıyla programlar makinaların okuyabileceği formatta hazırlanarak dağıtılmalıdır.

91. Denetçiler, bölümlere ayrılmış sistemlere itibar etmeyi düşünüyorlarsa; girdi, işleme, çıktı ve sistem değişiklik kontrollerini belgelendirmelidirler.

92. Daha fazla rehberlik için: KH Bölüm II (1.1-1.5, 2.1-2.5) ve SAC Modül 6 Bölüm 1.

ALARM SİNYALLERİ

Alarm sinyalleri daha fazla denetim çalışması yapılmasını gerektirebilecek alanları belirten ipuçlarıdır.

ORTAK / KURUMSAL - HEDEFLER VE STRATEJİLER

Alarm Sinyalleri veya İpuçları	Sorunun Tanımı	Gerekli olan Kanıt	Kaynaklar
Ortak Bilişim Yönetimi/Bilişim Teknolojisi Hedefleri ve Stratejisi mevcut değil.	Ortak iş planını destekleyen bilişim teknolojisi hareket planından bir kişi sorumlu olmalıdır. Plan Hazine Kurulu Sekreterliğinin stratejik talimatlarını da ihtiva etmelidir. Kullanıcılar plana dahil edilmelidir. Bilişim teknolojisine ilişkin girişimleri onaylayacak ve öncelikleri belirleyecek bir İcra Kurulu bulunmalıdır.	Kurumun hedeflerinin ve bilişim yönetimi planının bir kopyası	SDK Modül 5 Bölüm 2 KH Bölüm I, II, III
Kurumsal bilişim teknolojisi politikaları mevcut değil.	Bu politikalara, yazılım ve donanımın elde edilmesi ve gücünün artırılması, sistemin belgelenmesi, bilgi güvenliği, bilgisayarın kişilerce kullanımı, faaliyetler, destek/geri kazanım ve beklenmedik durumlar dahil olmalıdır.	Politikaların ve ilgili belgelerin bir kopyası	Hazine Kurulu . Sekreterliği Bilişim Yönetimi/Bilişim Teknolojisi Politikası, KH Bölüm I, 1.2
Üst yönetim bilişim teknolojisinin örgütlenmesi ve mevcut girişimler konusunda eksik bilgilendirilmiş.	Üst yönetim sistem geliştirme girişimlerini desteklemelidir. İlgi eksikliği ya da kurum içi anlaşmazlık mevcut olabilir.	Bilişim teknolojisi icra toplantılarının, diğer bilişim teknolojisi toplantılarının tutanakları, sistemler için alınan kararların kayıtları, iç yazışma	KH Bölüm I, 1.1 SDK Modül 5 Bölüm 2
Kapsamlı bilişim teknolojisi şeması veya mevcut sistemlerin şeması mevcut değil, belgelendirme zayıf veya az	Hızlı teknoloji değişikliklerinin anlatılması gerekiyor. Şemalar bu iş için idealdir. Belgelemenin mevcut olmayışı bilişim teknolojisi personeli ile kullanıcılar arasındaki iletişimin zayıf olduğuna işaret etmektedir.	Bilişim teknolojisi yapılanma şeması, sistem şemaları, yazılım ve donanım	SDK Modül 5 Bölüm 3

MÜŞTERİYE HİZMET

Alarm Sinyalleri veya İpuçları	Sorunun Tanımı	Gerekli Olan Kanıt	Kaynaklar
Kullanıcı komiteleri mevcut değil.	Kullanıcı komiteleri bilişim teknolojisi girişimleri için geri besleme halkası görevi görürler; program yöneticileri sisteme sahip çıkmada isteksiz olabilirler.	Toplantıları saptayın ve bunların tutanaklarını elde edin.	SDK Modül 5 Bölüm 2 KH Bölüm I, 2.2
Kullanıcı tatmininin periyodik ölçümü yapılmıyor. (araştırmalar)	Bilişim teknolojisi bölümü, kullanıcı topluluğuna ne derecede iyi hizmet verdiğinin farkında olmalıdır. İhtiyaçları en az iki yılda bir araştırın.	Araştırma anketlerinin bir kopyasını bulun.	SDK Modül 4 Bölüm 3 KH Bölüm I, 1.4
Kullanıcıların durumu, şikayetlerin haklı olduğunu göstermektedir.	Eğitimin ve sistem kurma yöntemlerinin ve zayıflığı, doğrudan telefon desteğinin olmaması, sorunların bildirilmesinde ve geri beslemede eksikliklere neden olabilir.	Kullanıcı destek yöntemleri	SDK Modül 4 Bölüm 3 KH Bölüm I, 1.4
Sistem geliştirme sürecine resmi kullanıcılar dahil edilmemiş	Kullanıcılar iş ihtiyaçlarını yönlendirmeli ve uygulamanın oluşturulması sürecinin bir parçası haline gelmelidirler.	Kullanıcı grubu toplantılarının tutanakları, şikayet yazışmaları	

BİLİŞİM YÖNETİMİ VE TEKNOLOJİSİ MALİYETLERİ

Alarm Singalleri Veya İpuçları	Sorunun Tanımı	Gerekli Olan Kanıt	Kaynak
Hali hazırda, kesinleşmiş bir bilişim teknolojisi maliyet / bütçeleme yöntemi mevcut değil.	Bilişim teknolojisi bölümleri; bakım faaliyetleri ve yeni sistemlerin geliştirilmesi için gerekli olan toplam maliyetleri her an bilmelidirler.	Bilişim Yönetimi sürecinin uygulanışı ve gerçekleştirilmesi ile ilgili maliyetleri elde edin.	Nelms, Elektronik Bilgi İşlem Dergisi, Cilt 3 (1992), syf. 72
Kurumun, sistem geliştirme maliyetleri bilgisi zayıf (kayıtlar).	Ya bilişim teknolojisi bölümünde ya da ilgili bölümde, proje yönetiminde zayıflık var.	Proje gözetim metodolojisini ve aylıklar da dahil olmak üzere proje maliyetlerini elde edin.	SDK Modül 4 Bölüm 2, 3
Yakın geçmişte bilişim teknolojisi maliyetlerine ilişkin olarak karşılaştırmalı bir çalışma yapılmamış.	Bilişim teknolojisi faaliyetlerinin bir çoğunun; maliyetlerin azaltılması veya verimliliğin arttırılabilmesi için özel sektöre devredilmeleri konusu incelemeye alınmalı.	Bilişim teknolojisi bölümü için yapılmış olan ya da iç denetim birimi tarafından gerçekleştirilen çalışmaları elde edin.	
Maliyet fazlalıkları, proje gecikmeleri.	Proje planlamasının veya proje yönetiminin zayıflığına işaret edebilir.	Maliyet hesaplarını ve gecikmelerinin ne gibi etkilerinin olduğunu kaydedin.	

BİLİŞİM YÖNETİMİ VE TEKNOLOJİSİ FONKSİYONUNUN YÖNETİMİ

Alarm Sinyalleri veya İpuçları	Sorunun Tanımı	Gerekli Olan Kanıt	Kaynak
Hazine Kurulu politikalarına ve standartlarına uyumda zayıflık.	Büyük projelere onay alınmadan başlanmış, stratejik yönelimler dikkate alınmamış, işletmeci yaklaşımı benimsenmemiş.	Hazine Kurulu Sekreterliğinin politikasının izlendiğini gösteren belgeler veya çalışmalar, Hazine Kurulu Sekreterliğinin mütalaaları.	Hazine Kurulu Sekreterliği Bilişim Yönetimi / Bilişim Teknolojisi Politikası.
Titiz bir çalışma ve gerekçe olmaksızın işleme anlayışında önemli değişiklik.	Merkezi işleme yönteminden, bölümlere ayrılmış işleme yöntemine geçiş, veri tabanı ve dosyalama sisteminde değişiklikler, telekomünikasyona daha fazla güven duyulması.	Kontrolların tanımlanması, kontrolların, iş akış şemalarının ve diğer belgelerin test edilmesi.	
Bilişim teknolojisi personelinde, proje yönetiminde ve süreçlerde sık sık yapılan değişiklikler	Hernekadar teknoloji süratle değişse de yapılan işi destekleyen sistemler hakkındaki bilginin sürekli olması gerekmektedir.	Kurum şemaları, olayların kronolojisi, kullanıcı şikayetleri	Amerikan Sayıştayı Bilişim Teknolojisi Sempozyumu
Bilişim teknolojisi personelinden geçerli bilgi almakta güçlükler	Tecrübeli ve bilgili personelin olmayışı, bilişim teknolojisinin ve kullanıcı kaynaklarının verimsiz kullanımına yol açar.	Bilgi istemlerine verilen yetersiz cevaplar	
Bilişim teknolojisi personeli ve kullanıcılar için eğitim planı mevcut değil.	Kullanıcılar ve bilişim teknolojisi personeli işlerini doğru bir biçimde yapabilmeli ve daha iyi nasıl yapabilecekleri konusunda bilgilendirilmeli.	Kursa katılım kayıtları, alınan eğitimin üretilen işle kıyaslanması.	KH Bölüm 1, 1.3
Kurumun, belli bir sistem geliştirme yaklaşımı yok.	Büyük sistemler yaşam dönemi çevrimi (life cycle) metodolojisi uygulanmaksızın geliştirilirler.	Planlama belgelerinin veya geliştirme yöntemlerinin olmaması veya bunların birbirleriyle çelişmesi.	KH Bölüm 1, 2.1-2.7
Sistem ve kullanıcı belgelenmesi çok az yada mevcut değil.	Sistem ve tesislerin işletilebilmesi için, ileri seviyeli bir belgeleme sisteminin mümkün olduğunca muhafazası gerekir.	Sistem tanımları, kullanıcı rehberleri, Hazine Kurulu Sekreterliği mütalaaları.	SDK Modül 5 Bölüm 4
Görev dağılımı iyi yapılmamış.	Yeterli kontrol yöntemlerini sürdürebilmek için; kullanıcı işlevlerinin programlama işlevinden ve faaliyetlerden ayrı sürdürülmesi gerekir. Kullanıcı sistemleri, genellikle bunu sağlayamadığı için denetçinin kararını kendi vermesi gerekecektir.	Kontrol akış şeması, sistem tanımları, muhtemel sorunlara ilişkin risk analizi.	KH Bölüm 1, 1.3 SDK Modül 4 Bölüm 2

BİLİŞİM GÜVENLİĞİ

Alarm Sinyalleri veya İpuçları	Sorunun Tanımı	Gerekli olan Kanıt	Kaynak
Bilgi güvenliğinden hiç kimse sorumlu değil.	Veriler, programlar ve donanım, olumsuz etkilerden ve izinsiz girişlerden korunmalıdır.	Tehlike ve risk değerlendirmelerinin , beklenmedik durum olay planları, kritik sistemler listesinin eksikliği.	Hazine Kurulu Sekreterliği Güvenlik Politikası SDK Modül 9 Bölüm 2 Datapro Bilişim. Güvenliği Auerbach 73-10-50
Sistem kayıpları göz önünde bulundurularak hazırlanmış ve işlemenin ve faaliyetlerinin sürekliliğini sağlayacak test edilmiş bir plan mevcut değil.	Plan; tehlike ve riskleri, beklenmedik durumlar karşısında izlenecek süreci, sorumlulukları, sağlanan fiziksel korumayı, önemli yazılımın tekrar kazanılmasını, programları, bilgi dosyalarını, formları, belgelendirmeyi ve kurum dışı depolama tesislerini ihtiva eder.	Beklenmedik durum planı ve test sonuçları, çalışmalara yeniden başlama planı.	Hazine Kurulu Sekreterliği Güvenlik Politikası KH Bölüm I 3.4-3.5 SDK Modül 10 Bölümler 2, 3 ve 6
Sistem ve verilerin destek ve geri kazanımı yönteminin bulunması ihtimali zayıf.	Veri ve program destekleri, sistemlerin önemi ve bilginin yeniden elde edilmesi maliyeti göz önünde bulundurularak yapılmalıdır.	Faaliyet süreçleri ve destek faaliyetlerine ilişkin kopyalar.	SDK Modül 4 Bölüm 3 KH Bölüm I 3.4-3.5
Yakın geçmişte güvenlik, tehlike ve risk değerlendirmeleri yapılmamış.	Hizmet içi yazılım kopyasının; orjinal program ve belgelerin, manyetik veya optik araçların; sistem girişlerinde donanımı güvenliğinin sağlanması amacıyla periyodik olarak incelenmesi gerekir.	Site değerlendirme raporları, teftiş raporları, iç denetim raporları.	Hazine Kurulu Sekreterliği Güvenlik Politikası SDK Modül 10 Bölüm 3
Şifrelerin veya şifre olanaklarının kullanımı paylaşılmıyor.	Kontrolların gevşekliği ihtimali, görev dağılımının iyi yapılmaması, sistem girişinde problem yaratabilecek iş tanımları (son sistem menüsünün araştırma memuruna verilmiş olması)	Şifre sistemi değerlendirme yöntemleri, kullanıcı giriş profilleri	KH Bölüm I 3.4 SDK Modül 9 Bölüm 4
Güvenliğe dikkat programı yok.	Kurum personeli; virüs bulaşmasından, destek taleplerinden ve sınıflandırılmış bilgi için gereken genel güvenlik önlemlerinden haberdar olmalıdır.	Prosedür el kitabının, güvenlik kurslarının veya haber bültenlerinin mevcut olmaması.	Hazine Kurulu Sekreterliği Güvenlik Politikası SDK Modül 9 Bölüm 2

TELEKOMÜNİKASYON

Alarm Sinyalleri veya İpuçları	Sorunun Tanımı	Gerekli olan Kanıt	Kaynak
Telekomünikasyonun veya yerel bölge bilgi ağlarının yeni kurulması.	Bölümlere ayrılmış sisteme ilişkin sorunlara ilave olarak, giriş ve izinsiz giriş kontrolları da değerlendirilmelidir.	Şifre kontrol profilleri, bilgı ağı topolojileri, modem giriş noktaları için kontrolların tesbiti.	KH Bölüm I 2.1-2.5 SDK Modül 8 Bölüm 2, 8
Elektronik bilgi değişimine başmanılması, yöneticilerden ziyade idari personelin elektronik belgeleri onaylaması.	İşlemlerle ilgili kayıt mevcut değil. Mali Yönetim Kanunu ve iç politika ile öngörülenler elektronik imzalar hariç, işlemlerin kağıda dökülmüş kaydı yok.	Sistem yetkilerinin listesi, sistemin detaylı bir şekilde genel değerlendirmesi, elektronik imza için gerekli kontrolların tesbiti.	Bilişim Yönetimi / Bilişim Teknolojisi Politikası Bölüm 3 Kısım 2
Tesis edilen hatlar için gelen faturaların ayrıntılı bir şekilde dökümü yok.	Tahsis edilmiş hatlar çok pahalı. Kullanımları izlenmeli. Faturalar kullanımı yansıtmalıdır.	Faturaları değerlendirmek amacıyla kullanılacak yöntemler.	
Yakın geçmişte, telekomünikasyon ihtiyaçları değerlendirilmemiş.	Veri trafik hacmi değişken. Bunların kullanımı izlenmeli. Yönetim, kiralanan hatlar ve teçhizatların envanterini takip etmelidir.	Telekomünikasyon çalışma raporları	SDK Modül 8 Bölüm 2

EKLER

1) Bilişim Teknolojisi Denetçisinin Yetenekleri

2) Yeni Çıkan Bilişim Teknolojileri

3) Bilişim Teknolojisi Yönetimi

EK 1 - BİLİŞİM TEKNOLOJİSİ DENETÇİSİNİN YETENEKLERİ

Denetim Kurumları bilişim yönetimi ve teknolojisini geçmişte olduğundan daha fazla kullanılmaktadırlar ve bu durum böylece devam edecektir. Denetim ekipleri, bilişim teknolojisi faaliyetlerini değerlendirebilecek bilgi ve yeteneğe sahip insan kaynaklarını elde etmeli veya bu kaynakları geliştirmelidirler. Kurum bünyesinde denetim grupları yada ekipleri oluştururken, bu kişilerde olması gereken yeteneklerin tesbiti önemli bir konudur. İdeal olarak, adayların sistem kontrol şeması çalışmaları yapmış olmaları, bilişim teknolojisi jargonunu bilmeleri ve muhasebe, maliye ve işletme konularında birikime sahip olmaları gerekmektedir.

Denetçinin Bilgisayar Destekli Denetim Teknikleri ile yapılan testler nedeniyle güvenilirliğin pekişeceğinin, denetime duyulan itimadın artacağının ve denetim maliyetlerinin azalacağının bilincinde olması gerekir. Denetçi ayrıca veri yönlendirilmesini ve yazılımdan örnekleme alınmasını bilmeli ve belirli bir sistemden alınan bilginin örnekleme için uygun olup olmadığını belirleyebilmelidir. Bu, veri toplama amacıyla denetlenen kurumdan nelerin istenebileceğinin bilinmesi anlamına gelmektedir. Denetçi yeni çıkan teknolojilerin faydaları yanında denetimin sorunları ve iş sürecinin yeniden tasarlanması konusunda da bilgi sahibi olmalıdır. Bilişim teknolojisi denetçisi kurumun faaliyetlerini anlamalı ve bilişim teknolojisi "taleplerini" kullanıcıların bilişim teknolojisi "ihtiyaçlarından" ayırabilecek analitik yeteneklere sahip olmalıdır. Denetçi yardıma ihtiyacı olduğunda Sorumlu Faaliyet Liderinin desteğini isteyebileceği durumları da saptayabilmelidir. Daha fazla bilgi için: SDK Modül 3 "Denetimde Bilişim Teknolojisinin Kullanılması", Auerbach 72-01-10, 73-01-10, 73-02-20, ve 73-02-50.

EK 2 - YENİ ÇIKAN BİLİŞİM TEKNOLOJİLERİ

Yeni bilgisayar teknolojilerinin kullanılmaya başlanmasının kurum üzerinde etkisi olmaktadır. Kişisel bilgisayarlar ve küresel teknolojiyi kullanan yerel sistem dosyaları, teknolojiyi kurumlardan ziyade kişilerin emrine sunmaktadır. Kurumlar; elektronik postayı, hesaplama tablolarını, özel uygulama yazılımlarını kullanan, yerel bilgi ağı uzmanlarını istihdam etmek suretiyle daha sade bir görünüm kazanmaktadırlar.

Günümüzde anabilgisayarlar, minibilgisayarlar ve mikrobilgisayarlar arasındaki fark, bunların kuruma olan genel maliyetleri arasındaki fark kadar net değildir. Küçük bir kişisel bilgisayarın donanım masrafı, yüksek bir eğitim giderine ve tahmin edilemiyecek bir destek maliyetine dönüşebilir. İlk etapta yüksek maliyetli gibi görünen bir anabilgisayar sistem yaklaşımı, bölümlere ayrılmış sistemin birim maliyetinden daha az bir maliyete sahip olabilir. Bunların herbirinin müşteri ve hizmetle ilişkilendirilmesi gereken avantajları ve dezavantajları vardır. Genel olarak anabilgisayarlar ve mini bilgisayarlar; birden fazla kullanıcı, birçok çevresel teçhizat, önceden tasarlanmış uygulamalar ve yöntemler, iyi bir şekilde hazırlanmış bir altyapı ve yüksek donanım ve yazılım maliyeti anlamına gelmektedir. Diğer yandan bir mikrobilgisayar; bilgisayara giriş hakkında veya programlar üzerinde çok az hakimiyeti olan tek bir şahıs tarafından da kullanılabilir. Denetçi için, kullanılan bilişim teknolojisinin mahiyetini ve bu teknolojinin uygulanışı ve kullanılmasının taşıdığı riskleri tesbit edebilmek önemlidir. Daha fazla bilgi SDK Modül 11, "Yeni Çıkan Teknolojiler"de bulunabilir.

Bölümlere Ayrılan veya Paylaşılan İşleme

Minibilgisayarlar ve mikrobilgisayarlardaki güç, bir uygulamanın birden fazla sistemde bulunacağı ve her birinin belirli işlemleri veya işlemlerin bir bölümünü işleyeceği ortaklaşa işleme ("bölümlere ayrılan işleme" ve "hizmet alan/hizmet veren" olarak da tanımlanmaktadır.) doğru bir yönelişe neden olmaktadır. Bunun kurum için birçok avantajlarının yanısıra riski de vardır. Sistem tasarlayıcısı bir uygulamayı tasarlarken her bir ortamın avantajlarını dikkate alabilir. Dolayısıyla birbiriyle bağlantılı yerleşik anaçerçeveler ortak bir bilgi temelini desteklerken bölümlere ayrılan işlemeler de hesaplamaları, incelemeleri, raporları ve araştırmaları destekleyeceklerdir. Avantajları ise asgariye indirilmiş anaçerçeve ihtiyaçları, genişletilmiş iletişim olanakları, kullanıcıya daha fazla hitap eden yazılımlar (interfaces), genellikle daha süratli olan gelişme süreçleri ve "kullanıcıya göre oluşturulan" sonuçlardır. Müşteri/verici yaklaşımının dezavantajları ise gerçekleştirme ve faaliyet maliyetlerinin daha fazla olması ve sistem bozulmalarına daha açık olmasıdır.

Ortaklaşa işlemenin; veri bütünlüğü ve doğruluğu, hataların düzeltilmesi, denetim izleri ve muhtemel belgeleme ve mutabakat sorunları gibi tasdik denetimine ilişkin bazı riskleri de bulunmaktadır. Kapsamlı denetime ilişkin riskler ise; maliyette artma ve eksilmeler olması, veri güvenliğinin, kullanıcıların eğitiminin ve uzmanlaşmanın azalması, sistem cevap verme süresinin yavaşlaması ve bir sonraki kullanıcıya hitap etmeyebilecek şekilde kullanıcıya göre hazırlanmış sonuçların sözkonusu olması şeklinde sıralanabilir. Hizmet alan/hizmet veren teknolojisinde en büyük sorun; PC-LAN'ların, "bunların daha büyük çaplı sistemlerle mukayesesinde, uygulama sistemlerinin fazla verimli olmaması"ndan dolayı maliyet konusunun ortaya çıkışıdır. (Gartner Grubu, Aralık 1993).

Ortaklaşa işleme "dışarıya kaynak ayırma" (iş verme) ile aynı şey değildir. Dışarıya iş verme; kurumun kendisini bilgi işleme tesislerinin ve kaynaklarının tümünden veya bir kısmından soyutladığı zaman gerçekleşir. İşi yüklenen kişi, sabit veya iş hacmine göre belirlenecek olan bir ücret karşılığında işlemeleri gerçekleştirmek için gerekli olan tesisleri sağlar. Bu ortaklaşa yada bölümlere ayrılan işlemenin gerçekleşmesine engel teşkil etmez. Dışarıya iş vermenin amacı, en iyi şartlarda, bir yüklenici ile ortaklık kurarak iş yükünün azaltılması, rekabet ortamının yaratılması, faaliyet personeli ve sistem faaliyet uzmanlarından birlikte yararlanmak suretiyle faaliyet maliyetlerinin azaltılmasıdır. Dışarıya iş verme ile ilgili riskler, dış kaynaklı veri merkezlerinin kullanılması ile genellikle aynıdır. Dışarıya iş verildiği durumlarda, Denetçinin bunun genel veri bütünlüğü ve işleme maliyetleri üzerindeki kısa ve uzun vadeli etkilerini de bilmesi gerekmektedir.

Telekomünikasyon

Günümüzün iletişim teknolojilerinde, büyük miktarlarda bilgiyi aynı anda taşıyabilen fiber optik kablolar sayesinde; görüntünün elde edilmesi, bütünleşmiş ses ve veriye daha hızlı bir şekilde ulaşım ve bulma hizmetleri gerçekleştirilerek daha fazla kişiye ulaşma imkanı sağlanmaktadır.

Telekomünikasyon şirketleri, fazla kalite kaybı olmaksızın, 24 dijital ses sinyalini tek bir bilgi kanalına sıkıştırabilmektedirler. Rekabetin artması nedeniyle iletişim maliyetleri sürekli olarak azalmaktadır. Bu, daha ucuz kiralama ücretlerine yol açmakta ve kurumlara, daha yüksek iletişim ücretleri ile sağlayamayacakları online hizmetleri sunarak müşteri hizmetlerini büyütme imkanı vermektedir.

Elektronik veri değişimi ile elektronik imzalar ve fon onayına ilişkin protokollerin kullanılmasını kolaylaştıracak bir takım standart kamu faaliyeti formatları kullanılmaya başlanmıştır. Hükümet, bilgiyi birçok kurum ve teknolojiler ile paylaşabilmek amacıyla bir "Süper Bilgi Otoyolu" oluşturmaktadır. Bu projenin ismi, Araştırma Endüstrisi ve Eğitimin Geliştirilmesi İçin Kanada Bilgi Ağı'dır (CANARIE). Teknoloji mevcut olmasına rağmen bunun ne şekilde kullanılacağı kesin olarak bilinmemektedir. Bunun uzun vadede, bölgesel ofisleri bulunan büyük kuruluşların denetimine etkisi olabileceği düşünülmektedir.

Denetçi için telekomünikasyon birçok risk içermektedir. Kullanımı pahalıdır ve yanlış kullanılması da kuruma pahalıya mal olabilir. Dışarıya, diğer bir deyişle iletişim taşıyıcılarına devredilen ve bilişim teknolojisi idarecileri tarafından çok iyi anlaşılamayan bir uzmanlık alanıdır. Daha da önemlisi, ortak veri tabanlarına yasa dışı girişlere olanak sağlayan bir yöntemdir. Eğer kurum, hayati önem taşıyan sistemleri için telekomünikasyona güveniyorsa; telekomünikasyon idaresi ve yönetimi, bilgi ağı güvenliği ve bütünlüğü, iletişim kiralama ve teçhizat maliyetleri ve destek ile geri kazanım planlarının değerlendirilmesinde dikkatli olunmalıdır.

Veri Saklama Teknolojisi

Geçen yıllarda, bilgisayarlardaki bilgilerin saklanmasında, manyetik saklama en önemli elektronik yöntem olmuştur. Ancak, artık optik bilgi saklama manyetik yöntemin yerine geçebilecek uygun, süratli ve yüksek kapasiteli bir seçenek olarak karşımıza çıkmaktadır. Birçok avantajı olmasına karşın, optik teçhizatın küçük ve taşınabilir (disketler gibi) olmasından dolayı hırsızlık ve bilginin açıklanması riskini de taşımaktadır.

Veri Tabanı Teknolojileri

Fiziksel olarak bölümlere ayrılmış bir çok veri tabanından yararlanabilen gelişmiş veri tabanı yönetimi sistemlerinin kullanımıyla bir çok soruya cevap alınabilir ve bilginin nerede bulunduğunu ve fiziksel olarak nasıl düzenlendiğini bilme gereği duyulmadan raporlar hazırlanabilir. Verinin birden fazla uygulama sistemi aracılığıyla kullanılması ve paylaşılması; kullanıcıların çoğunun uygulama sistemleri ve veri toplama yöntemleri üzerinde yapılan ve veri bütünlüğü, güncelliği ve doğruluğuna ilişkin kontroller konusunda az veya hiç bilgiye sahip olmamaları nedeniyle mevcut olan riski arttırmaktadır.

Ayrıca denetçi, veri güncelliği ve mevcut verilerin yetkisiz kullanım ya da değiştirilmelere karşı korunamilmesi için kullanılan fiziki ve mantıksal güvenlik önlemleri konularında da bilgi sahibi olmalıdır. Denetçi, kurum tarafından kullanılmakta olan destek/geri kazanım yöntemlerini ve kurum için hayati önem taşıyan ve (test edilmiş) işe yeniden başlama planlarını bilmelidir. Bu sistemlerden alınan bilginin doğruluğunun teyidi, örnekleme yapmak veya program değerlendirme bilgisi toplamak isteyen denetçi için çok önemlidir.

Uzmanlık Sistemleri

Uzmanlık sistemleri (veya bilgi temelli sistemler), sorunları çözmek için bilgiyi ve netice çıkarma kurallarını kullanan üstün nitelikli bilgisayar sistemleridir. Tipik bir uzmanlık sistemde aşağıda belirtilen unsurlar bulunmaktadır: muhtemel sorunları çözmek için gerekli olan bir uzmanlık bilgi temeli; işlemleri kurallara tatbik ederek netice çıkarabilecek bir sistem yada program ve girdileri ile kabul ederek sonuç çıkartabilecek bir buluşma sistemi. İlk uzmanlık sistemleri tıbbi teşhislere ve diğer basit karar verme uygulamalarına yardımcı olmak amacıyla tasarlanmışlardır. Uzmanlık sistemleri sahteciliğin saptanması için de kullanılabilir (Laplante, A., *Bilgi Dünyası*, Ocak 1993). Hükümet bu tür sistemleri, Gelir Güvenliğinin Yeniden Tasarımı projesinde kullanmayı düşünmektedir. Denetçi açısından; veri bütünlüğü ve doğruluğuna ilişkin riskler bulunmaktadır. Bilgi temelinin sürdürülmesi ve doğruluğunun sağlanması amacıyla sık sık güncelleştirme yapılması gerekir. Hükümet ve bakanlık politikalarının birçok özelliği bilgisayar programlarına yansıtılmıştır. Bu mantıki yapıların istenmeyen müdahelelerden korunması korunması amacıyla sistem yakından gözlenmelidir.

Yeni Çıkan Diğer Teknolojiler

Kamu işyerlerine hergün yeni ürünler girmektedir. Örneğin, denetçiler yakında multi medya teknolojisine dayanan hükümet sistemleriyle karşılaşacaklardır. Bunlarda elektronik kalem kullanacağı gibi görüntüleme ve grafiklerde, lazer disk teknolojisinin yüksek bilgi kapasitesi desteği de olacaktır. Bu teknolojilerde, ses tanıma yazılımı tarafından harakete geçirilecek ve kişisel video konferansında kullanılacak video telefonu da mevcuttur. Yakın gelecekte kişilerin yaşantısına ilişkin bilgi saklayacak ve sosyal hizmetlere yardımcı olacak "akıllı kartın" daha fazla kullanılmasını bekleyebiliriz. Yeni "grup yazılımları" grup kararlarını pekiştirmek amacıyla kullanılmaktadır. "Satış noktası" sistemine birçok yönden benzemekte olan "sözleşme sistemleri noktası"nın kullanımı artmaktadır. Böylelikle, orta seviyedeki yönetimin müdahalesi, işbaşındakilerin sorumluluğunun ve hizmet düzeyinin arttırılmasıyla ortadan kalkmış olacaktır.

Yukarıda belirtilen teknolojilerin kullanımının ortak özelliği, işlem akışını takip edecek geleneksel yöntemlerin yok olmasıdır. Günümüzün elektronik bilgi alışverişinde de olduğu gibi denetçiler; kurumsal ve yasal usullerin gereken şekilde takip edilip edilmediğini saptayabilmek için, kurumlar arasındaki (satıcı, müşteri, banka, ve diğer üçüncü şahıslar) elektronik işlemleri ve imzaları yeniden yapılandırabilecek bir yazılımı kullanabilmeli ya da yaratabilmelidir.

Bu yeni teknolojiler kamu kuruluşlarına girdikçe denetçiler bunların risklerini ve kontrollerdeki etkilerini değerlendirmeye devam etmek durumundadırlar. Denetçiler de, denetim amaçları için benzer araçları kullanabilirler.

EK - BİLİŞİM TEKNOLOJİSİ YÖNETİMİ

Federal hükümet dahilinde, bilişim teknolojisi yönetimi bakanlıkların sorumluluk alanları içindedir. Harcama limitleri ve Hazine Kurulu Sekreterliği talimatları çerçevesinde; bakanlıklar belirtilen şekilde hizmetlerini yerine getirebilmek için istedikleri sistemi kurma ve kendi işlerini verimli, etkin ve hesaplı bir biçimde idare etme özgürlüğüne sahiptir. Bilişim Yönetimi, Sistemleri ve Teknolojisi Başkanlığı ve alt komiteleri vasıtasıyla Hazine Kurulu Sekreterliği politikalar oluşturur ve rehberlik sağlar. Aşağıda sunulan bölümler bu komitelerin her birinin çalışmalarını ve birbirleriyle olan ilişkilerini anlatmaktadır.

Bilişim Yönetimi, Sistemleri ve Teknolojisi Başkanlığı

Haziran 1993 tarihinde hükümet, Hazine Kurulunda Bilişim Yönetimi, Sistemleri ve Teknolojisinden sorumlu Bilişim Yöneticisi makamını oluşturmuştur. Bilişim Yöneticisi bilişim teknolojisi ve bununla ilgili telekomünikasyon politikalarını geliştirir. Bilişim Yöneticisi, bilişim teknolojisi grubu ile fonksiyonel olarak bağlantılıdır. Bilişim teknolojisi bölümleri kendi bakanlık yapılarına göre rapor hazırlamaya devam ederlerken; bir derece kadar merkezden yönlendirme, standardizasyon ve düzeltici önlemler sağlayabilmek ve olayların yakından incelenmesi suretiyle üretilen politikalar bağlamında hükümet çapında bir diyaloğun oluşturulması amaçlanmaktadır.

Bilişim Yöneticisi, Hazine Kurulu Sekreterliğinin "90'lar için Stratejik Hedefler" (Hazine Kurulu Sekreterliği, *Hizmetlerin Pekiştirilmesi*, 1992) teklifini onaylamıştır. Bu programı oluşturan beş unsur şöyledir: hükümet kurumlarındaki hizmetlerin ve program faaliyetlerinin yenilenmesi; işletmeci yaklaşımını kullanarak yatırımlar yapmak; diğer bakanlıklar ve özel sektör ile ortaklıklar kurmak; çekirdek altyapı ve bilişim teknolojisi için açık bir altyapı inşaa etmek; ve bilgisayar imkanlarını idarecilere ve personele ulaştırmak.

Gelecekte Bilişim Yöneticisinin, daha önce Sayıştayın üstlendiği danışmanlık rolü dışında işlerle daha direkt olarak ilgilenmesi beklenmektedir. Bilişim Yöneticisi geçtiğimiz iki yıldan beri İdari Yenileme Konseyinin yapmakta olduğu çalışmaları sürdürdüğü gibi kamu idaresinin yeniden yapılanması faaliyetlerini yönetmektedir. Seçilen işlevler yeniden yapılandırılırken bakanlıklardan finansman ve insan kaynağı ve satın alma alanlarında ortak sistemler geliştirmeleri istenmektedir.

Bilişim Yöneticisi, kamuya elektronik hizmet ulaştırılmasının uygulamaya konması konusunda bakanlıklara yardım sağlamak amacıyla bir çerçeve oluşturacaktır. Gizlilik, kişisel kimlik numarası gibi sorunlarda bütün bakanlıklar adına hükümet çapında bir yaklaşıma ihtiyaç duyulmaktadır.

Bilişim Yönetimi, Sistemleri ve Teknolojileri Komitesinin Yapısı

Bilişim Yönetimi, Sistemleri ve Teknolojileri kamudaki bilişim teknolojisi gruplarına uygun olan ve bunların ulaşabilecekleri politika ve rehberliği geliştirmek amacıyla birçok komite oluşturmuştur. Her birinin kısa bir tanımı aşağıda sunulmaktadır:

- Hazine Bilişim Yönetimi Komitesi: Bilişim Yönetimi Alt Komitesi ile ilgilenen Hazine Kurulu Üst Danışma Komitesi; politika teklifleri, üzerinde durulacak sorunlar, projelerin sponsorluğu ve hükümet çapındaki Bilişim Yönetimi, Sistemleri ve Teknolojileri planları konularında, Bilişim Yöneticisi aracılığıyla Hazine Kurulu Sekreterine tavsiyelerde bulunan müsteşarlardan oluşmaktadır.

- Bilişim Yönetimi Danışma Komitesi: Bilişim Yönetimi Danışma Komitesi bakanlıkların üst düzey bilişim teknolojisi yöneticilerinden oluşmaktadır. Ana teknik danışma grubudur ve Komite başkanı Bilişim Yöneticisidir.

- İdari Yenileme Komitesi: İdari Yenileme Komitesi bakanlıkların değişik bölümlerinden gelen çok sayıda üst düzey yöneticilerden oluşmaktadır, örneğin: personel, finansman insan kaynağı ve satın alma. İdari Yenileme Komitesi hükümette yönetimsel verimlilik sağlanması için çalışan bir kullanıcılar forumudur.

Kurumsal Bilişim Teknolojisi Sorumlulukları

Bilişim Yönetimi, Sistemleri ve Teknolojisine benzer bir şekilde kurumların da merkezi sistemleri, güvenlik ve telekomünikasyon planlamaları ve performans sorumlulukları bulunmaktadır.

Kurumsal Bilişim Teknolojisi Politikaları ve Standartları

Kurumlar, Hazine Kurulu Sekreterliğine bilişim yönetimi ve güvenlik politikalarını nasıl hayata geçireceklerini belirtmek zorundadırlar. Yazılım ve donanımların elde edilmesi ve kullanımı için kurum standartları ve rehberlik yöntemleri oluşturmaları gerekir. Bilişim teknolojisi bölümü izlenecek asgari politikaları ve yöntemleri oluşturmalıdır (örneğin belgeleme, programların test edilmesi vs.). İlaveten, kurumlar bilişim güvenliği politikaları ve bilinçlenme programları hazırlamalıdırlar.

Veri Yönetimi. Kurumlar, nerede bulunursa bulunsunlar, ortak verilerin tamamının bütünlüğünü, güvenli bir şekilde saklanmasını ve desteklenmesini sağlamalıdırlar.

Sistem Gelişimi. Kurumlar kurum için, küçük yada büyük, yeni sistemlerin geliştirilmesinin koordinasyonundan sorumludurlar. Çoğu zaman, merkezi dosyaları güncelleştiren ortak sistemlerin geliştirilmesi, genellikle veri girişi ve araştırma programlarından oluşan ve bölgelerde uygulanmakta olanlardan daha farklıdır.

Sistemlerin Sürdürülmesi. Kurumlar mevcut sistemlere ve bunlarla ilgili belgelendirmeye süregelen desteği muhafaza etmek zorundadırlar. Sistemler faaliyet ihtiyaçlarına uygun bir şekilde güncelleştirilmelidir. (Bu mevcut sistemlerin daha etkili hale getirilmesi ve bunların sağladığı faydalardan tekrar tekrar yararlanılması.)

Eğitim. Kurumlar uygun iletişim araçları ve eğitim planları vasıtasıyla, bilişim teknolojisi personelini, yeni veya geliştirilmekte olan sistem olanakları konusunda bilgilendirmelidirler. Kurumlar mikrobilgisayar desteği ve eğitiminin kullanıcılara açık olmasını sağlamalıdırlar. Yeni çıkan teknolojileri takip edilmeli ve kullanıcılara bu konuda tavsiye ve danışmanlıkta bulunulmalıdır.

Telekomünikasyon Desteği. Kurumlar mikrobilgisayarları, yerel bilgi ağlarını ve bilgi merkezlerini birbirine bağlayacak iletişim otoyolunu veya "iletişimin belkemiği"ni düzenlemek zorundadırlar. Gereken olduğu durumlarda, dış kaynaklı veri tabanlarına da geçiş sağlamak durumundadırlar. İletişim maliyetlerinin düşük tutulması amacıyla sık sık iletişim ihtiyaçlarını gözden geçirmelidirler.

Bilişim Güvenliği Planlaması. Kurumlar tehlike ve risk değerlendirmeleri yapmalı ve görev için hayati önem taşıyan sistemleri belirlemelidir. Yukarıda da belirtildiği gibi bilginin korunması ve saklanması amacıyla sorumlulukları tarif eden bir güvenlik politikasına sahip olması gerekir. Tüm kurum için, işe yeniden başlama planı oluşturulmasının yanısıra, uygulama sistemleri destek/geri kazanım yöntemlerini de hazırlamalı ve test edilmelidir.

Kurumsal Üst Yönetim

Kurumun çalışma planı bir kere hazırlandıktan sonra; üst yönetimce bilişim teknolojisi çalışma vizyonunu destekleyen ve genel başarıya katkıda bulunan bilişim yönetimi planı geliştirilerek hayata geçirilmelidir. Üst yönetim, işe olan katkılarına göre bilişim teknolojisi önceliklerini belirlemek zorundadır. Üst yönetim, bilişim teknolojisi, bilgi değerlerinin yönetimi ve bilgi güvenliği ile ilgili olarak Bilişim Yöneticisi tarafından oluşturulan politikaları kurumda yerleştirmelidir.

Özetle, bilişim teknolojisinin kullanımı ve yerleştirilmesi ile ilgili planların, Hazine Kurulu Sekreterliği tarafından teklif edilen çerçeve dahilinde olması ve kurum amaçlarına uygun ve bu amaçları destekler nitelikte olmalarının sağlanması, üst düzey yönetimin çalışma alanına girmektedir.

Kurumsal Program Yöneticileri

Kurumun iş hedeflerini oluşturan veya talimatlarını yerine getiren program yöneticileri, sistemin esas kullanıcılarıdır ve çoğu zaman da yeni ihtiyaçların öncüleridir. Nihai ürünün iş ihtiyaçlarını gerçekten desteklediğinden emin olabilmek üzere sistemlerin ve teknolojinin tedarik ve kurulma aşamalarına dahil olmaları gerekmektedir. Ayrıca, sistemde kullanılan bilginin doğru ve tam olmasını sağlayarak kalite kontrol işlevini de yerine getirmektedirler.

Bilişim Teknolojisi Yöneticileri

Teknoloji değiştikçe bilişim teknolojisi yöneticisinin görevi de değişmektedir. Mikrobilgisayarların kullanılmaya başlanmasından sonra birçok geleneksel bilgi işleme yöntemi değişmiştir ve daha önce merkezden yapılan işler artık nihai kullanıcıların, yerel bilgi ağı yöneticilerinin veya bunların her ikisinin de sorumluluk alanına girmektedir.

Bilişim teknolojisi yöneticilerini bekleyen zorluk; merkezi ve yerel işlemeyi, kullanıcıların ihtiyaçlarına uygun olan bir sistem karışımı sağlayacak şekilde dengelemektir. Dolayısıyla bilişim teknolojisi sorumluluğu olan kişilerin kolayca adapte edilebilecek, kullanıma uygun ve kullanıcıların kolay ve ilgi çekici bulacağı teknolojileri sürekli olarak sunmaları gerekmektedir. Bu, artık geleneksel ana çerçeve (sera) yaklaşımı değildir. Kullanıcılar, artık bilişim teknolojisinin işlevlerinden daha fazlasını yerine getirmektedirler ve bu faaliyetlerin koordine edilmesi ve desteklenmesi amacıyla bilişim teknolojisi yöneticisinin görevini de genişletilmiştir.